Privacy Commissioner

Annual Report 1990-1991

ERRATA

Page 28 paragraph 2

The number of not well-founded complaints against the RCMP should read 66, not 16. The table on pages 32 and 33 is correct.

Annual Report
Privacy Commissioner
1990-91

91-05816/

The Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

(613) 995-2410, 1-800-267-0441
Fax (613) 995-1501

© Minister of Supply and Services Canada 1991

Cat. No. IP30-1/1991

ISBN 0-662-58483-X

The Honourable Guy Charbonneau
The Speaker
The Senate
Ottawa

June 28, 1991

Dear Mr. Charbonneau:

I have the honour to submit to Parliament my annual report. This report covers the period from April 1, 1990 to March 31, 1991.

Yours sincerely,

Bruce Phillips

Bruce Phillips
Privacy Commissioner

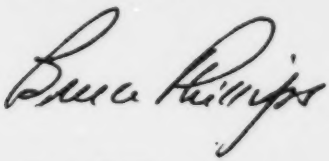
The Honourable John Fraser, P.C., Q.C., M.P.
The Speaker
The House of Commons
Ottawa

June 28, 1991

Dear Mr. Fraser:

I have the honour to submit to Parliament my annual report. This report covers the period from April 1, 1990 to March 31, 1991.

Yours sincerely,



Bruce Phillips
Privacy Commissioner

Table of Contents

Mandate 1

New conductor, familiar score 2

Privacy and the Charter 8

Cellular phones and privacy 13

Privacy in the private sector 15

Biomedical testing 18

Electoral reform—a permanent voters' list 22

Privacy and the public interest: a difficult balance 24

Complaints directorate 26
- Directorate report 26
- Tables and charts 30
- Cases 35
- Notifying the Commissioner 44
- Policy and research 47
  - Data matching 47
  - Technology marches on 52
  - Consulting the Commissioner 54
- Inquiries 55

Compliance directorate 57

Corporate management 61

Organization chart 63

Mandate

The *Privacy Act* provides individuals with access to their personal information held by the federal government; it protects individuals' privacy by limiting those who may see the information; and it gives individuals some control over the government's collection and use of the information.

The Act sets out the principles of fair information practices, requiring government to :

- collect only the information needed to operate its programs;
- collect the information directly from the individual concerned, whenever possible;
- tell the individual how it will be used;
- keep the information long enough to ensure an individual access; and
- "take all reasonable steps" to ensure its accuracy and completeness.

Individuals in Canada may complain to the Privacy Commissioner if:

- they are denied any part of the information;
- they are denied their request to correct some of the information on the file— or their right to annotate it;
- the department takes longer than the initial 30 days or maximum 60 days to provide the information;
- the **Info Source** description of the contents of the information bank is deficient in some way;
- the department's listing in the Source does not describe all the uses it makes of personal information;
- an institution is collecting, keeping, using or disposing of personal information in a way which contravenes the *Privacy Act*.

The Privacy Commissioner's investigators examine any file (including those in closed banks) except confidences of the Queen's Privy Council to ensure that government institutions are complying with the Act.

The Act also gives the Privacy Commissioner the power to audit the way government institutions are collecting, using and disposing of personal information.

New Conductor, Familiar Score

This is the first annual report to Parliament in eight years to be submitted by anyone other than John Grace who, until June, 1990, was the sole person to have served as Privacy Commissioner of Canada since the office was established as a function separate from the Canadian Human Rights Commission in 1983.

Mr. Grace completed his term of office in July of 1990 and assumed new duties as Canada's Information Commissioner. He departed this office with a high reputation in several respects: first, as an ombudsman with an outstanding gift for resolving privacy problems and complaints; second, as an energetic and eloquent spokesman for the cause of protection of personal privacy, and third, as the respected leader of a small but highly-motivated staff of skilled investigators and auditors who reflected his abiding concern for this vital but embattled area of human rights.

He also was ever alert to the new challenges to privacy protection which continue to arise with almost bewildering rapidity and number in a constantly-changing commercial and technological environment.

Thus Mr. Grace has bequeathed to his successor the advantage of a smoothly-functioning organization. Many of the issues touched upon in this report were initiated prior to Mr. Grace's departure.

During the interval between the departure of the former commissioner and the confirmation of a new one, a period of some ten months, the duties of acting commissioner were performed by the executive director, Alan Leadbeater. He served with distinction in the difficult dual role of both administrative head and ombudsman.

The new commissioner, coming into office almost on the eve of this report, is acting in some senses as a surrogate spokesperson for two predecessors, although he was, as assistant commissioner, the beneficiary of their experienced counsel and guidance. In fact, the ten months expended as assistant commissioner proved to be an invaluable introductory exposure to a field which is both complex and becoming more so. If the reader detects any diffidence in the tone of the observations, be assured it is attributable to the realization that the author still has much to learn.

It may be small comfort to this neophyte that he is not alone. In fact, the privacy guard also changed in Ontario and Quebec during the year. Paul-André Comeau was appointed Quebec's new Access and Privacy Commissioner and Thomas Wright was named Information and Privacy Commissioner of Ontario. One thing should not change—the cordial and mutually supportive relationship among these offices.

This report, in attempting to give a reading on the state of privacy protection in the nation, will share with its predecessors something of the quality of a "good news-bad news" story. It is the nature of the issue that there will be no final victories. Personal privacy is a problem intimately bound up with the relationship of the individual to society, and so long as society continues to evolve and change, so too will the problems affecting privacy.

There is no more fragile, yet important, right in today's complex society than the right to a reasonable expectation of privacy. It is not a right, which some cynics suggest, that only serves those with something to hide. Without a meaningful measure of privacy our fundamental freedoms of expression, belief and association risk becoming meaningless.

Justice Brandeis, in his famous 1898 definition of privacy as "the right to be let alone", could not have contemplated a world of ingenious machines with unlimited capacity for collecting, collating and transmitting information across global networks. Nor could he have foreseen a science capable of plumbing the deepest secrets of human heredity.

The right to be left entirely alone, if it ever existed, could now be exercised, if at all, only, in the farthest corner of the most remote reaches of our arctic. Even then, one suspects, the putative recluse would sooner or later see some indomitable servant of a government department looming over the frozen horizon bearing the all-important form which, when properly filled out, would confer that indisputable certification of human existence, a Social Insurance Number.

But if absolute privacy in modern society is neither attainable, practical nor even particularly desirable, the struggle must continue to preserve the individual's right to decide the degree to which personal privacy is to be sacrificed on behalf of other competing rights and claims.

So the notion of an annual fever-chart, while it provides a convenient method of keeping score, is to a certain extent misleading unless it is clearly understood that, wnere privacy is concerned, the patient will always be in danger since it is under assault from new afflictions as rapidly as remedies for older ones are found.

One is struck by this phenomenon in reading past annual reports. Many of the issues which dominate privacy discussions today were barely in the privacy vocabulary eight short years ago. For example there is drug testing, AIDS testing, and implications of genetic research, interception of cellular telephone communications, to name but a few, and some of which will be referred to later in this report. Doubtless this will continue to be the experience in future, since there is no reason to believe there will be any relaxation in the onward march of science and technology. The best one can do is to stand firmly on the privacy ramparts, trying to dam the breaches as they occur, and confident of nothing except that it will be a never-ending struggle.

So how did the struggle proceed in the year just past?

Certainly there is no reason on the available evidence to suppose there has been any abatement in the technological onslaught against personal privacy. Computers continue to proliferate (80,000 in the possession of the federal government alone, at last estimate), the tide of junk mail continues to mount, the commercial trafficking in personal information continues to increase (a $3 billion annual business in the U.S., and, presumably, on the usual proportion, at least $300 million in Canada).

But, on the proposition that an aroused and informed public is the best bulwark of privacy rights, there are very positive signs of real and lasting gains.

In the marketplace

Past reports have referred to the growing awareness of invasive marketing practices in the private sector. In 1990, the issue received the final accolade of media stardom—a TIME Magazine cover story. And although some of the participants might have wished otherwise, further proof of the rising profile of privacy issues emerged in the political arena in two provinces where ministers found themselves in difficulties over disclosures which, in two cases at least, led to a resignation. Whatever else one might think or say about them, these events underline that privacy rights cannot always be ignored with impunity. And, if the marketplace in recent years has generated some of the major threats to privacy, the marketplace acting in self-interest in the end may also prove to be at least partly a self-correcting mechanism.

Presumably in response to growing consumer concern, the private sector is showing (at long last, some might say) encouraging signs of action. During the past year, the Canadian Bankers Association, Bell Canada and the Canadian Direct Marketing Association have all produced codes offering significant improvements in the protection for privacy and confidentiality of information concerning their clients. These developments are discussed in more detail later in the report, but here it is worth noting that they offer some hope yet for the path of voluntary action.

The issue now is not whether the private sector can continue without privacy codes, but how long it will be before compulsion in one form or another enters the equation. Thanks to developments in Europe, North American business may soon lose its ability to engage in data transfers with European business unless it has privacy codes in place. This development lends added urgency to the Commissioner's recommendation to Parliament last year that the *Privacy Act* be amended to require all federally-regulated private sector firms to implement privacy codes based on internationally-accepted guidelines and principles.

Even assuming such voluntary codes become a feature of the Canadian marketplace, there remains a question about their effectiveness. Highly-respected authorities believe some form of oversight is necessary before business becomes truly accountable to the public for protecting privacy.

Dr. David Flaherty, the leading Canadian academic in the field of privacy research, argues that a federal audit power is required to ensure private sector compliance with its own voluntary codes. His is a view which must be respected, yet the Commissioner continues to hope (as did his predecessor) that such a degree of intervention (with the massive resources it implies) may be forestalled by the private sector demonstrating some good privacy citizenship.

Certainly there remains a long way to go. Citing one small example, some chartered banks in their credit card applications still include in the fine print virtual absolute waivers of the privacy rights of customers. These waivers confer upon the banks the right to re-use, in any way they see fit, any or all of the information provided, such as salary, employment history, personal assets and in one case, the Social Insurance Number. A few sharp-eyed consumers have noted these waivers and drawn them to the attention of this office but most, we suspect, did not notice. Such fine-print caveats do not meet any reasonable definition of "informed consent". Neither do they reflect the spirit of enhanced respect for privacy to which the chartered banks' own association now lays claim.

On the positive side, the Canadian Direct Marketing Association is commended for providing a process by which consumers may have their names removed from the mailing lists of their members. Since the association covers more than 80 per cent of the firms engaged in direct marketing, this is a forward step.

Still, such modest improvements are in no way keeping pace with the exploding volume of information exchange made possible by the computer. Thus a minimum step to imposing some standards on the trade in personal information should be the introduction of a legislated requirement that all business under federal jurisdiction implement approved privacy codes. The Commissioner considers this urgent.

Also needed is for Parliament to restore privacy to telephone communications in Canada, now eroding with the spread of cellular telephones. Cellular communications can and are being intercepted by easily available monitoring equipment. There seems no reason why the absence of conventional wires should deprive customers of the right and expectation of privacy. Sale or possession of monitoring equipment should be limited to authorized organizations for use only in conformity with laws governing surveillance activities.

Appraising the manager

Readers of last year's report may recall the Commissioner's cool reception of a proposed hotline for anonymous tips from public servants about government fraud, waste and mismanagement. Happily the idea was dropped.

But many of the same privacy problems are inherent in a new management tool departments are taking up with enthusiasm—"reverse" or "upward" appraisals. As the terms imply, the process allows employees to evaluate their managers' performance anonymously. Although it has been used by large private sector corporations, this is a novelty for government agencies which, as part of public service reform, now design their own appraisal systems.

The process requires employees to complete a questionnaire, rating managers on their management skills and personal traits. The completed forms then are analyzed, sometimes by a private consultant, and summarized. Managers receive a copy but do not see individual employees' ratings or comments.

There are several privacy problems in the process—first is promising employees confidentiality to prevent reprisals. The *Privacy Act* gives individuals the right to see what others say or write about them. And so promising confidentiality to employees who complete the appraisals is misleading and hollow.

In contrast, it is firmly established public service practice for employees to review, comment on and even (if they wish) appeal managers' appraisals of their performance.

Second, the notion that privacy rights can be sidestepped by contracting out the process is dangerous and unsupportable. To accept such a view would mean that all government privacy objectives could be foresworn by turning personal information over to private contractors. The implications go well beyond concern that managers would lose their right of access and that the Act would not protect this highly personal information from improper use or disclosure. However, once hired, contractors are agents of the government and it retains "control" of the information, wherever it happens to be stored.

Few would argue with government's aim to improve management and accountability. But establishing a process which subverts its own legislation is hardly the proper weapon.

A year at the office

As it has in almost every year since the office was established, the number of complaints, investigations, and audits has increased. Although the details are compiled in separate chapters elsewhere in this report, the office is now working at full stretch and, general restraint notwithstanding, Honorable Members and Senators must understand that the obligations they have laid on the office under the *Privacy Act* can not be discharged at their present level of efficiency by the existing modest staff of 34 persons. Investigations now number more than 1,200 a year, exceeding 100 per investigator. Any significant increase in this workload, which experience suggests is inevitable, simply cannot occur without sacrificing existing standards of service.

The compliance branch also had a busy year, but it is worth noting that after eight years of operation, it has managed audits in only about one-fifth of the 150 federal departments and agencies covered by the *Privacy Act*. Clearly, if the reach of the Act is ever extended to include audit responsibilities in the private sector, the existing compliance branch of nine persons will be unequal to the task.

On the research side, the major effort of the office during the previous year was a study of the privacy implications of drug testing. The study found that mandatory random drug-testing in the workplace was unjustified, and in some circumstances, probably illegal. The office notes with approval that the Department of Transport has modified to some extent its drug-testing plans, but disapproves of the Department of National Defence and at least one chartered bank going forward with drug-testing programs which constitute unwarranted breaches of personal privacy. This issue is discussed in greater detail in a separate chapter.

Now in the final stages of preparation is a study on the implications of progress in genetic research and testing, a subject which holds the promise of even greater privacy problems than drug-testing. The report is expected to be published in late summer of 1991.

Privacy and the Charter

It is both fascinating and gratifying for a Privacy Commissioner to watch the Supreme Court of Canada fashion a prominent place for the right to privacy within the *Canadian Charter of Rights and Freedoms*. It is fascinating for the ups and downs of the saga — and gratifying for the overall growing strength of the right to privacy.

Two previous annual reports followed this unfolding study. There is more to tell this year.

On September 11, 1983, police seized 278 pounds of marijuana from a vehicle and charged a number of individuals with conspiracy to import an illegal substance. The Crown's case was based on 136 phone calls intercepted during an intensive investigation in widely separated areas of British Columbia.

The police believed that the alleged conspirators used public pay telephones to conduct their affairs and so they installed listening devices on 20 public pay phones. Tape recorders were attached to pay phones on some 20 occasions and left on automatic record overnight, intercepting and recording conversations of suspects and others. While the police obtained judicial authorizations for these wiretaps, none of the authorizations specifically allowed the bugging of pay phones. Rather, the authorizations employed a "basket clause" giving police the authority to intercept communications at certain addresses and "...elsewhere in the Province of British Columbia resorted to by (the suspects)...".

The trial judge ruled that, in these circumstances, the judicial authorizations were invalid. In his view, the automatic monitoring of public pay phones when such monitoring is not specifically authorized by a judge, permits a dragnet type of investigation not contemplated by the *Criminal Code*. He ruled the intercepted communication inadmissible and directed the jury to acquit the accused.

The B.C. Court of Appeal saw it differently, reversed the trial judge's decision and ordered a new trial. The Court of Appeal concluded that it was not necessary for the authorization to make specific reference to pay phones as long as any monitoring of pay phones was not indiscriminate. The Court of Appeal found that an intercepted communication itself could (by containing a suspect's voice) provide evidence that the monitoring was not indiscriminate.

The Supreme Court of Canada resolved the matter in a 4-2 decision, *Thompson, et al* v. *The Queen*, issued October 18, 1990. The Supreme Court conclusion is most interesting, if puzzling.

Writing for the majority, Justice Sopinka concluded that the "basket clause" authorization was lawful even though no mention was made of public pay phones nor were any limiting conditions imposed to protect the public. However, he wondered whether the interceptions which took place in this case pursuant to the valid authorizations were "reasonable" under section 8 of the *Charter*.

He concluded that in at least four instances, taps were placed on public pay phones solely because they were near where a suspect was staying and that this was insufficient evidence to act upon. "...(it) amounts to little more than indiscriminate monitoring based on a hunch" (p. 26). Furthermore, since this jeopardized the right to privacy of innocent third parties (hundreds of private conversations may have been intercepted when not one target was involved), Justice Sopinka concluded that it infringed upon section 8 of the *Charter*.

Now the puzzling part. Justice Sopinka reasoned that it would not bring the administration of justice into disrepute to admit the evidence obtained from wiretapped public pay phones. Consequently, the appeal was dismissed and a new trial ordered.

What comfort does this give us? Strong admonitions are made against relying on the "basket clauses" in wiretap authorizations. Judges and the police are strongly encouraged by the Court to minimize the intrusions upon the privacy of innocent third parties when seeking or granting wiretap authorizations and when intercepting communications. Yet, the law enforcement community is essentially told that if it fails to live up to these standards, no matter — their cases will not be jeopardized.

The dissenting opinions of Justice La Forest and Justice Wilson point out the shortcomings in the thinking of the majority. Both said that since the tapping of public pay phones give rise, *per se*, to massive violations of privacy, judicial authorizations for such activity must be expressly made and not granted by implication under the "resort to" basket clause. By not taking this view, the Supreme Court has left it to Parliament to ensure that *Charter* infringements are not perpetrated by the police. How completely the respective roles of the *Charter* and Parliament have been turned. Justice La Forest puts it eloquently:

> "It will be obvious that the Act (*Criminal Code*) and the *Charter* place a heavy burden on the courts to ensure the privacy of Canadians. Electronic surveillance is indiscriminately acquisitive; its reach extends to the conversations of the innocent and the guilty alike. The indiscriminate acquisitiveness of electronic surveillance invites the courts to redouble their vigilance and to be especially sensitive of the potential of certain practices to undermine the expectation of Canadians that their private communications are inviolable. This legitimate and reasonable expectation of privacy will not long survive if the courts give their *imprimatur* to practices that allow the police to intercept private communications solely on the basis of their own reasonable belief that valuable evidence stands to be gained thereby. In my view, 'resorted to' clauses can easily result in the application of this low threshold and constitute the 'fishing expeditions of considerable latitude' decried by this

court in *Hunter* v. *Southam*, *supra*, at p. 167. It is sad to reflect that, even with the assistance of the *Charter*, the courts have failed to take the steps necessary to avoid this danger and that if Canadians are to receive adequate protection against the insidious threat to individual privacy posed by electronic surveillance, they must turn to Parliament to provide additional safeguards. There is biting irony in this. The *Charter* was designed to protect us from possible inroads on individual rights by Parliament". (pp. 13-14)

And so, a Privacy Commissioner, at best, has mixed emotions about the *Thompson* decision. We must applaud the Court's new insistence that, when police intercept private communications, the privacy rights of innocent third parties must be protected. There is a strong message to judges and the police to be especially vigilant when wiretaps are installed at places frequented by the public. Although the Court does not make it a mandatory requirement, it suggests that visual surveillance accompany the wiretap to ensure that only a suspect's conversations are intercepted. Canadians should be comforted by the Supreme Court's consciousness of privacy threats to innocent parties when police engage in wiretapping. Nevertheless, the Court also makes it clear that if Canadians are to be adequately protected against these abuses, Parliament must act to strengthen the wiretap provisions of the *Criminal Code*.

Therefore, the Privacy Commissioner urges the government to propose, and Parliament to enact, measures necessary to ensure adequate control of wiretapping practices.

This year's Supreme Court privacy story, however, does not end with a whimper. Its decision in the case of *Santiago Wong* v. *The Queen* (November 22, 1990) is a bang.

The *Wong* case resulted from a Toronto police gambling investigation conducted during the summer of 1984. The security staff of a major downtown hotel told police they suspected that hotel premises were being used for illegal gambling. There was evidence of gambling in a recently vacated hotel room and the police learned that the person who had reserved the room, Mr. Wong, had also reserved it for later the same month.

The police installed a video camera in the room with the permission of the hotel management but without judicial authorization or warrant. Activities in the room were monitored on five separate occasions and resulted in charges being laid against Mr. Wong and ten others for keeping a common gaming house.

The trial judge found that the video surveillance was an infringement of section 8 of the *Charter* and dismissed all charges. The Ontario Court of Appeal, however, noted that invitations had been widely circulated within the Chinese community and that strangers who came to the hotel room were welcomed. In these circumstances, the court found that the accused had no reasonable expectation of privacy and that, as a result, section 8 of the *Charter* did not apply. A new trial was ordered.

On appeal the Supreme Court, in a 6-1 decision, took a different view. It concluded that without judicial authorization, such video surveillance was an infringement of the section 8 protection against unreasonable search and seizure. This decision is especially remarkable because it extends the privacy right to a right to freedom from indiscriminate video surveillance by agents of the state. The Court concluded that this privacy right must be protected by an independent judiciary and that police cannot be left to decide when video surveillance may be employed.

In his majority judgment, Justice La Forest is clear that all forms of electronic surveillance by agencies of the state, not judicially authorized, violate section 8 of the *Charter*.

> "...the broad and general right to be secure from unreasonable search and seizure guaranteed by s. 8 is meant to keep pace with technological development, and, accordingly, to ensure that we are ever protected against unauthorized intrusions upon our privacy by agents of the state, whatever technical forms the means of invasion may take." (p. 6)

As a result of *Wong*, it is no longer appropriate for a court to inquire into whether a person who is the subject of unauthorized surveillance has "courted the risk".

In Justice La Forest's words:

> "...privacy would be inadequately protected if an assessment of the reasonableness of a given expectation of privacy were made to rest on a consideration whether the person concerned had courted the risk of electronic surveillance. In view of the advanced state of surveillance technology, this would be to adopt a meaningless standard, for, in the final analysis, the technical resources which agents of the state have at their disposal ensure that we now run the risk of having our words recorded virtually every time we speak to another human being." (p. 7)

Thus, despite the fact that the accused had widely issued invitations to his hotel room and opened the door to strangers, he did not lose his right to a reasonable expectation of privacy. The Court made it clear that while we might impose warrantless video surveillance on those who engage in illegal activities in their hotel rooms, society would object to imposing that risk on anyone who rents rooms. In order to avoid the latter, the Court considered that it must prohibit the former.

Unlike wiretapping, there is currently no available procedure for police to obtain a judicial authorization for video surveillance. The Court was fully aware of the handicap its decision imposed upon the police, but felt that only Parliament should decide the circumstances in which the police could invade privacy by means of video surveillance.

In Justice La Forest's words:

> "On my view of the matter the courts would be forgetting their role as guardians of our fundamental liberties if they were to usurp the role of Parliament and purport to give their sanction to video surveillance by adopting for that purpose a code of procedure dealing with an altogether different surveillance technology. It is for Parliament, and Parliament alone, to set out the conditions under which law enforcement agencies may employ video surveillance technology in their fight against crime. Moreover, the same holds true for any other technology which the progress of science places at the disposal of the state in the years to come." (p. 22)

No doubt the government will introduce legislation to provide for the judicial authorization of video surveillance by the police. That would be the responsible course since no one questions the need for video surveillance in law enforcement. However, as with wiretapping, the Privacy Commissioner urges Parliament to ensure that any process for obtaining judicial authorization for video surveillance protects the privacy of innocent parties.

Cellular Phones and Privacy

In the past year Canadians have become aware—some painfully so—that cellular telephone calls can be intercepted.

One British Columbia cabinet minister resigned after a newspaper printed extracts from calls he made on his car phone. Some provincial delegations at the Meech Lake Conference suspected that their cellular communications had been intercepted. And a provincial power corporation was embarrassed when someone intercepted and published an employee's comments about third parties during a cellular phone conversation.

Faced with this troubling new threat to privacy, the Commissioner has tackled two questions:

- Does the *Privacy Act* protect cellular phone calls?
- And do federal government institutions, including its law enforcement agencies, only intercept cellular communications in compliance with the law?

The Supreme Court decisions (discussed above) make it clear that, without proper judicial authorization, agencies of the state may not subject individuals to any form of electronic surveillance. To do so would be "improper search and seizure". It would sacrifice our right to a reasonable expectation of privacy, thus infringing section 8 of the *Charter of Rights and Freedoms*.

The state may no longer assume that individuals have waived their right to privacy just because they "court the risk" of surveillance by, for example, using a communications technology known to be vulnerable to interception. According to the Supreme Court, that assumption would incur a greater risk—that electronic surveillance without a proper warrant would so dilute our privacy as to be inconsistent with a free and open society.

That conclusion has direct implications for the *Privacy Act*. The Act controls the collection of personal information by federal institutions. Principal among these controls is one which prohibits collecting personal information "...unless it relates directly to an operating program or activity of the institution" (section 4).

This provision is open to interpretation in specific cases. But it cannot be read to sanction a collection of personal information which would otherwise be unlawful. Collecting personal information in a way which violates the Charter would also breach the *Privacy Act*.

Since the *Privacy Act* is implicated when federal investigative bodies intercept cellular calls, the Privacy Commissioner wants to satisfy himself that any federal interceptions comply with the Act. However, the emphasis is on fact-finding. There is no reason to believe that federal authorities are unlawfully invading the privacy of Canadians' cellular phone calls.

The commissioner is making inquiries and anticipates reporting the results in next year's annual report.

More troubling is the absence of any legal control over private citizens intercepting cellular phone calls. As one commentator puts it:

> "While the average cellular telephone user may be prepared to contend with occasionally finding another conversation sharing his line, he may be concerned to discover that conversations can be deliberately monitored using something as simple as an old TV set capable of receiving cellular UHF frequency".(**Network Newsletter,** Vol. 10, No. 24, July 30, 1990, p.1)

Using the *Charter*, the Supreme Court has cobbled together protections against cellular monitoring by agents of the state, but the *Charter* does not control individuals' behaviour. And it is doubtful whether current *Criminal Code* provisions prohibiting the surreptitious interception of private communications apply to cellular phone calls. After all, a cellular communication is carried on radio waves and so may not be considered "private".

Some other jurisdictions—California, for example—have passed laws prohibiting both interception of cellular calls and the sale or purchase of cellular eavesdropping devices. An even broader law is before the U.S. Congress covering computer communications and radio communications (H.R.3378 and S.1667). That proposal would make it unlawful to eavesdrop on a car phone conversation or any other private radio communication.

Of course, laws in themselves cannot ensure that cellular conversations remain private. In fact, some argue that such laws could lull cellular phone users into a false sense of security and, hence, be counterproductive. The Commissioner does not agree. It is vital for Parliament to act quickly to protect the privacy of cellular phone users. The mere disappearance of the wires which once carried our communications must not end in the disappearance of our privacy.

Privacy in the Private Sector

In a highly computerized society information knows no boundaries. Yet Canada contents itself with an information policy which distinguishes between the government and the private sector. There is some legal protection against information abuses in the federal (and some provincial) public sectors. But there are no controls over the private sector.

In Europe, the situation is markedly different. Most member countries of the European Community (EEC) have imposed data protection controls over both the public and private sectors. And Europeans are strengthening and harmonizing these controls as they plan for a unified Europe in 1992.

These developments have significant implications for Canadian firms doing business in Europe—or which hope to. Without comparable data protection laws in Canada's private sector, European countries may no longer allow companies to transfer their citizens' information to Canada. In effect, European data protection laws could become a non-tariff barrier, seriously hampering Canadian firms in their dealings with what promises to be one of the strongest trading blocks in the world.

This is no idle fear. In July 1990 the EEC issued a draft directive on protecting individuals' personal data. If adopted, it would bind all EEC member countries on January 1, 1993. The directive is designed to accomplish two broad goals.

- The first is to establish a uniform, high level of privacy protection in both the public and private sectors.
- The second is to remove all barriers to the free flow of personal data among member countries.

The directive has alarming implications for non-EEC member countries which do not measure up to the European standards. Article 24 of the draft requires members not to transfer personal data to any jurisdiction which does not ensure the data adequate protection. Given current Canadian law, it is unlikely that the private sector could prove that it adequately protects personal data.

All relevant European authorities—the OECD, the Council of Europe, the EEC and European data protectors—are fully aware of the directives's implications for countries which are not EEC members. They know that Canada (and the U.S., too) endorses data protection principles (Canada has signed the OECD Guidelines on the Protection of Personal Information). And they know that North America prefers to let the private sector police itself through voluntary compliance. But the Europeans also know that voluntary compliance has not proved particularly successful. In both Canada and the U.S. only a handful of private firms have established meaningful data protection codes of practice.

And so, while the Europeans have been willing to accept that there may be more than one way to ensure adequate data protection (voluntary codes among them), they are unwilling to compromise on the principle. There must be meaningful protection. European data protectors, the guardians of their citizens' privacy, will no longer agree to risk it by authorizing transfers of personal data to countries that pay only lip-service to data protection.

This is not a prediction hazarded on a whim. It is a summation of the comments of several European data protectors to the Privacy Commissioner.

In last year's annual report, the Privacy Commissioner recommended that Parliament amend the *Privacy Act* to require federally-regulated private sector firms to develop, file and implement privacy codes based on the internationally accepted principles established in the OECD Guidelines.

From his discussions with European data protectors the Commissioner believes voluntary codes would be acceptable—as long as they had this statutory underpinning.

Therefore, the Commissioner considers action on this recommendation is urgent. Not only do Canadians deserve this much privacy protection but, without it, Canadian firms risk labouring under a significant competitive disadvantage in their post-1992 dealings with Europe.

Hopeful beginnings

Private sector success stories should not be treated lightly simply because they are few in number. A case in point: in December 1990 the Canadian Bankers' Association (CBA) approved a model privacy code containing the minimum data protection standards member banks must apply to their customers' information.

The code provides customers with rights of access to and correction of their information. As well, it controls the banks' collection, retention, use, disclosure, disposal and security of customer records. Banks have an admirable success record in protecting customer confidentiality but now the code will give their customers greater control over their financial information.

Privacy advocates (the Commissioner among them) will find flaws. One that stands out is the code's failure to provide customers with access rights to recorded opinions or judgements about them. Only factual information will be available. Nor will the code protect employees. Nevertheless, CBA's adoption of a code must be applauded.

Another success story is Bell Canada, the largest telecommunications public utility. It too has adopted a privacy code. However, the Bell code grants privacy rights and protections to employees as well as customers. And access rights are not limited to factual data.

In an increasingly competitive telecommunications environment, Bell's tangible sensitivity to its customers' and employees' privacy is bound to have a ripple effect. The Commissioner urges other telecommunications companies to follow suit. He will monitor and report their progress.

Finally, important new privacy protections were recently announced by the Canadian Direct Marketing Association (CDMA). On February 13, 1991, CDMA launched its "Operation Integrity". CDMA has strengthened the privacy protections in its code of ethics, committing itself to giving consumers greater control over unwanted intrusions by direct mailers and telemarketers.

The program requires all CDMA members to allow consumers to opt out of their mail and phone lists. In addition, members must not include sensitive medical, financial, insurance or court information in the lists they rent. Finally, CDMA has established a task force of senior industry officials to study the privacy impications of direct marketing and to develop additional policies on transferring data.

Operation Integrity is an important step towards ensuring consumers' privacy is respected. The Privacy Commissioner appreciates CDMA's courtesy in keeping him informed and looks forward to continuing this dialogue.

Biomedical Testing

Drug testing

Regular readers of these reports will recall last year's strong cautions against resorting to widespread drug testing to wage the "war on drugs" in the federal government.

The Commissioner's in-depth study—**Drug Testing and Privacy**—examined several environments - transportation, prisons, the armed forces and athletics. Many testing programs being contemplated by the government risked violating the *Privacy Act*, the *Charter of Rights* or broader notions of the individual's integrity.

Clearly there has been some movement to protect privacy interests threatened by drug testing. The office has been consulted by Health and Welfare about drug testing protocols. It has responded to the federal government's report on drug testing in transportation. And it has discussed with the Correctional Service of Canada (CSC) its proposed regulations on drug testing in federal penitentiaries.

Transport Canada no longer proposes to conduct random mandatory drug testing for those in safety-sensitive positions. CSC's proposed regulations are an improvement over earlier ones struck down in 1989 by the trial division of Federal Court in the **Jackson** case. Health and Welfare testing protocols now contain less intrusive means of taking urine samples than did earlier proposals.

Unfortunately there are elements of the transportation drug testing policy that remain troubling. Transport Canada still intends to impose urinalysis at the time of employment, transfer and during regular medicals although its own research revealed no serious threat to safety in the industry caused by substance use. As well, urinalysis provides very limited information—that a substance has been consumed in the past—but not how often or whether the employee was impaired or, more important, is **now** impaired. Mandatory drug testing in these circumstances offends the *Privacy Act* and might not survive a challenge based on the *Charter of Rights and Freedoms*. Urinalysis should be confined to testing "for cause" or after an accident.

Regrettably, National Defence remains committed to its proposal to impose drug tests on its members.This, despite the Commissioner's recommendations and the transport committee's conclusions about random mandatory testing. DND intends to test for cause, as part of an accident or incident investigation, during a probation period following a positive test result and for data collection. It also plans random mandatory tests of members in operational or safety-sensitive positions. Unfortunately, although DND has not yet begun testing, it remains committed to the program or a modified version of it.

There is yet another concern. Fitness and Amateur Sport responded to the Dubin report on drug use among amateur athletes by setting up a new anti-doping organization funded primarily by—but not part of—the federal government. The organization will co-ordinate all sport anti-doping programs in Canada and conduct an expanded program of testing athletes for banned substances.

A major focus of the program would be "no-notice" testing of athletes outside of competition. Up to 3,000 tests could be conducted (presumably annually), the majority of which would be no-notice.

Because the anti-doping organization will not be a federal agency, it will not be subject to the *Privacy Act*. This may have been a deliberate attempt to circumvent the Act. Nevertheless, the organization's approach (as announced by the minister) prompts some general privacy objections. Athletes may find themselves with precious few privacy rights. The Commissioner intends to discuss this situation with officials from Fitness and Amateur Sport.

The Commissioner continues to be concerned about the lack of merit of most drug testing programs. Little this office has seen in the past year has altered its thinking about the fundamental futility of testing programs and their inherent intrusiveness. The government's example is a poor one for the private sector to follow. In most cases, the programs now contemplated or introduced by government appear not to comply with the *Privacy Act*. But public criticism of these programs is the strongest weapon this office has. It cannot enforce compliance.

HIV testing

The office's principal work on HIV/AIDS was the 1989 report, **AIDS and the Privacy Act.** The office also contributed to developing the "Guidelines on Ethical and Legal Considerations in Anonymous Unlinked HIV Seroprevalence Research". The guidelines were developed through meetings arranged by the Federal Centre for AIDS in late 1988 and published in the **Canadian Medical Journal** in 1990. In February 1991 the office participated in a review of the original guidelines.

In November 1990 the Commissioner's office was represented at the meeting of the Council of International Organizations of the Medical Sciences (CIOMS), a World Health Organization body. The meeting discussed draft ethical guidelines on epidemiological research, including HIV/AIDS research. Staff continue to handle requests and investigate complaints about privacy and HIV/AIDS. Since the requests often concern issues or bodies not covered by the *Privacy Act*, the office attempts to re-direct callers to the appropriate authorities.

The office's work on HIV/AIDS is complemented by work in Ontario. The Ontario Law Reform Commission is doing a broad study on the legal (and, to some extent, ethical) implications of HIV/AIDS testing. The Ontario Information/Privacy Commissioner has published two reports on HIV/AIDS, one dealing with HIV/AIDS and privacy, the other with HIV/AIDS and the workplace.

Genetic testing

Genetic testing is just one of many evolving biotechnologies that pose serious privacy dilemmas. Genetic testing encompasses three techniques. The first—genetic screening—examines a tissue or blood sample from an individual for genes or genetic "markers" indicating a present or potential genetic disorder or other physical trait.

The second technique is genetic monitoring. It looks for genetic or chromosomal changes that may be caused by exposure to workplace or environmental chemicals or phenomena (radiation or the fumes from plastics, for example).

The third technique is forensic DNA analysis, sometimes colloquially (and inaccurately) referred to as DNA fingerprinting. This technique matches samples of material genetically. Blood stains from the scene of a crime may be genetically matched with those of a suspect. Forensic DNA analysis may also prove blood relationships in immigration or paternity cases.

Genetic technology holds great promise for the identification of genetic disorders, a limited number of which may be treatable. However, there is a privacy concern in the potential of genetic testing to reveal highly sensitive information about the person tested and his or her genetic relatives.

Other forms of biotechnological testing, such as screening for HIV/AIDS antibodies or drugs, reveal only a single piece of information—infection with the HIV or the past use of drugs. But genetic testing can reveal hundreds of bits of information about an individual or relative. The data ranges from the certainty of developing crippling or deadly diseases (such as Huntington's chorea or cystic fibrosis), to the likelihood of developing psychiatric disorders (manic depression) to predispositions to elevated cholesterol levels, high blood pressure or certain cancers.

Genetic testing is on the brink of becoming an issue in human reproduction (pre-conception, prenatal and neonatal testing), employment (screening and monitoring), access to government and private sector services (schooling, insurance, credit), criminal investigations, during ordinary medical care and in performing research.

The current and potential uses of the information produced by genetic testing persuaded the Commissioner to study its privacy implications. While its uses are now confined primarily to reproduction, its potential is enormous. Better that society examine the technology's implications before it attacks privacy rights. The study should be completed by late Spring 1991.

The Commissioner has always been loathe to press for regulation of the private sector. However, the privacy implications of genetic testing demand that the government consider whether there should be direct regulation of any private sector uses of this highly intrusive technology.

The Commissioner is not alone. Privacy experts are examining similar measures in the United States. Most western European countries already regulate personal data collection by the private sector. In this sense, Canada is falling behind a growing movement to protect individual privacy not only from governments, but from the seemingly insatiable curiosity of the private sector.

Electoral Reform - A Permanent Voters' List

Privacy issues can rear their heads where least expected. A case in point was the government's appointment of a Royal Commission to determine whether Canada's electoral laws needed overhauling.

The commission was asked to examine the electoral process and party and campaign financing and to study the option of a permanent voters' list that would replace door-to-door enumeration.

Doing away with costly, time consuming door-to-door enumeration may be appealing. The process contributes to the length and expense of Canadian federal elections, but the alternative needs serious study.

The commission heard proposals which focussed on combining data from such federal data banks as income tax files, citizenship information, change-of-address notices to Canada Post, census forms and pension records. Others proposals suggested incorporating provincial health and drivers' records and there was significant support for a voter's identity card or a requirement that voters produce a Social Insurance Number.

As a result, the Privacy Commissioner wrote to the commission asking it to consider the privacy impact of its recommendations.

His concerns included the implication of new large-scale collections (or linkages) of personal information. This type of permanent voters' list would become the sort of population register that could pose a real threat to human rights and freedom. Wartime experience proves that such lists will be abused—even in Canada—to subject large groups of individuals to discriminatory treatment, arrest, detention and confiscation of their property.

Further, once in place, pressures would mount to make the list widely available to all arms of government for unrelated uses. Ensuring exclusive election use and absolute confidentiality of the data would be vital.

Growing dissatisfaction with abuses of SIN reflects public resistance to national identification and registration schemes—a resistance which would be compounded if SINs were used to link the databases and to establish a citizen's right to vote.

Finally, the *Privacy Act* prohibits access to other federal data bases to create such a list. Thus, Parliament would have to pass legislation to override the *Privacy Act*, a step the Commissioner could never support.

Citizens around the world are fed up with being counted, recorded and monitored by the state. A voters' list could evoke deep unease. It would be ironic if the electoral process—the heart of the democratic way of life—became the vehicle which tipped the scales further from the individual to the state.

While the Commissioner does not want to restrict progress, he does want to ask some pertinent questions before the project advances too far. The electoral commission has welcomed his input and plans to report to the public in the fall of 1991.

Privacy and the Public Interest: a Difficult Balance

Generally the *Privacy Act* prohibits government institutions from disclosing personal information without the subject's consent. However, the Act also recognizes 13 circumstances which dispense with this rule.

One of the 13 is very general and, hence, both difficult to apply and easy to abuse. Sub-paragraph 8(2)(m)(i) authorizes disclosure without consent:

> "for any purpose where, in the opinion of the head of the institution,
> (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure..."

During the past year the most frequent user of this provision was Correctional Service of Canada (CSC). The situation develops when prison incidents such as escapes, unnatural deaths or hostage takings lead to internal investigations and subsequent reports. These reports contain personal information about both the inmates and prison officials who were involved. Consequently, CSC must consider the restrictions contained in the *Privacy Act* before disclosing the reports.

CSC may want to release the reports in order to preserve public confidence in the correctional system. It may also need to provide copies to journalists who have requested access under the *Access to Information Act* or to members of Parliament or Parliamentary committees wanting to review the reports to assess overall correctional administration. In these situations, CSC removes information which is exempt under the *Access to Information Act* as well as sensitive or extraneous personal details.

CSC seeks to disclose only sufficient personal information necessary to satisfy the public interest test set out in the *Privacy Act* and give the public a clear picture of what transpired.

Once this screening satisfies the commissioner of corrections and the solicitor general, they notify the Privacy Commissioner of the intended release, in advance if reasonably possible. When the Commissioner receives the notification, he assesses whether there is a public interest disclosure which clearly outweighs any resulting invasion of privacy. If he does not agree he tells the institution. However, the Commissioner has no power to prevent the release—only to tell the individuals affected that their information will be disclosed.

Evidence of just how difficult it is to apply the "public interest" test was demonstrated in two disclosures which the Commissioner reported last year ("Reports on two inmate escapes"). The Standing Committee on Justice and the Solicitor General wanted to inquire into the events surrounding the two widely-publicized prison incidents—the escape from Dorchester, New Brunswick, of Allan Légère (during which he allegedly murdered one person) and the day-pass release from the Edmonton institution of Daniel Gingras (during which he murdered two people).

CSC had previously disclosed censored versions of the investigation reports to the media and gave that version to the justice committee. The committee, however, wanted the uncensored versions and issued an order to the solicitor general for the complete reports.

The solicitor general refused to act on the order, maintaining that the *Privacy Act* prohibited the disclosure. His refusal became the subject of a question of privilege in the House of Commons and the matter was referred to the Standing Committee on Privileges and Elections.

In his testimony before the committee, the solicitor general held that he was responsible for respecting sub-paragraph 8(2)(m)(i) of the *Privacy Act*. Therefore he had to be satisfied that a public disclosure of the reports would be in the public interest and that this interest clearly outweighed any invasion of individual privacy. He did not believe that the *Privacy Act* gave him the authority to accede to the committee's demand for an in-camera review of the uncensored reports.

The then-acting Privacy Commissioner, appearing before the privileges committee, applauded the solicitor general's resolve to protect the privacy of persons mentioned in the reports. However, he felt that the minister was taking an unnecessarily narrow view. Sub-paragraph 8(2)(m)(i) of the *Privacy Act* clearly gives the solicitor general the authority to determine whether disclosure of the uncensored reports to an *in-camera* session of the Justice Committee is in the public interest. The acting Commissioner maintained that it was not at all inconsistent with the provision to decide that disclosure to the committee is in the public interest, providing it takes place under conditions which would ensure that the censored portions remain confidential.

At the time of this report, the final chapter of this story has yet to be written. The privileges committee has not concluded its deliberations and the Privacy Commissioner has not completed his investigation of a related complaint.

"The truth, the whole truth and nothing but the truth"

However, there is another facet to this story. It is unusual for the Privacy Commissioner to publicly remind government institutions that privacy is not an absolute value. But the Act does recognize that privacy may be invaded in order to serve certain important, collective goods.

Being doctrinaire in insisting on confidentiality in all cases risks giving the *Privacy Act* a bad name—one it does not deserve. These CSC incident reports are a case in point.

Although the public interest CSC wants to serve (by disclosing these reports) is public confidence in the corrections system, CSC has removed portions which are critical of correctional staff members. While CSC's action to shield these individuals may be understandable, it leads to a report which gives the public a less than complete picture of the incident.

Without giving the "bad" with the "good" can CSC really be serving the public "interest"? This question is the subject of ongoing discussion between CSC and the Privacy Commissioner. What is needed, it would seem, is for CSC to use the public interest clause as an extraordinary measure and, when it is invoked, to ensure that the disclosures give the complete picture.

Complaints Directorate

Complaints have increased by approximately 10 per cent per year since the office opened for business seven years ago. This year the pattern continued as the office received 1,239 complaints compared to 1,086 last year—a 14 per cent increase.

Time limit complaints

Occasionally the Commissioner felt like a stuck record during previous reports as comments about Correctional Service Canada and National Defence delays were a recurring theme.

Now, the music has changed. Time limit complaints were down substantially this year and full credit goes to Correctional Service Canada. CSC's response to the Commissioner's criticism of last year's performance was a complete overhaul of its request handling procedures.

The result was an astounding 200 per cent decrease in new CSC time limit complaints—from 214 last year to 50 this year. Last year's volume accounted for 50 per cent of the office's delay complaints. This year's total—only 15 per cent. A tip of the hat to Correctional Service for a job well done.

Another entrenched cause of delay complaints was the Department of National Defence handling of members' Personal Evaluation Reports (PERs). The problem occurred because military personnel had to make formal application to see their evaluations and the result was a huge caseload and an inevitable backlog. Last year the Commissioner applauded National Defence's decision to treat PERs requests informally. As predicted, the number of privacy requests to DND dropped 20 per cent — most of the decrease directly attributable to the policy change. The result is a 36 per cent decline in time limit complaints against National Defence—from 78 to 50.

Clearly, government institutions are trying hard to respect the statutory time limits, the trend is evidence of that. But shrinking resources threaten the "good news" story. An individual's right to timely access to personal information should not be sacrificed on the altar of fiscal restraint.

Fair information code

Although complaints about denial of access were up, this past year's 14 per cent hike results from a substantial jump in complaints about collection, use and disclosure of personal data—the fair information code. This year's complaints against the code skyrocketed to an unprecedented 386 from last year's total of 173.

Again, labour-management disputes at Canada Post Corporation seem to be at the root of the problem. The corporation appears to be administering its new leave management policy aggressively. Employees are concerned that medical information about them has been improperly collected and used to manage attendance at work.

Top ten

This year's report includes a list of the office's top ten clients, a group which accounts for 80 per cent of its total caseload. Correctional Service Canada, the perennial leader in the new complaints category until this year, has happily ceded that honour to Canada Post Corporation.

New complaints against Canada Post went from 97 to 237, while CSC's 165 are less than half of last year's record 392.

Another significant increase occurred at Employment and Immigration Canada where the 128 complaints represented a three-fold jump. Transport Canada has returned to a more characteristic total of 67 after a low of six complaints in 1989-90. For no apparent reason National Archives, National Defence and the Canadian Security Intelligence Service have also seen significant increases while Health and Welfare and the RCMP have experienced decreases.

		GROUNDS		
DEPARTMENT	TOTAL	ACCESS	TIME LIMITS	OTHER
Canada Post Corporation	239	40	54	145
Correctional Services Canada	165	77	50	38
National Defence	163	51	56	56
Employment and Immigration Canada	128	61	44	23
Canadian Security Intelligence Service	77	67	9	1
Revenue Canada, Taxation	75	23	39	13
Transport Canada	67	43	17	7
National Archives of Canada	51	12	1	38
Royal Canadian Mounted Police	50	35	2	13
Health and Welfare Canada	32	14	15	3
Others	192	95	50	47
TOTAL	1,239	518	337	384

How institutions measured up

A number of factors—such as an unexpected volume of requests—can prompt complaints. Actually, many of the factors are beyond the control of the institutions. A more meaningful performance indicator is the proportion of complaints that are well-founded.

Using this measure, the Royal Canadian Mounted Police is the most successful institution by a long shot. Only five complaints were well-founded (or well-founded/resolved) while 16 were not well-founded and seven were discontinued. This is a decrease from 19 well-founded complaints two years ago and 10 last year. This reflects the RCMP's sincere respect for the letter and spirit of the Act. But special kudos are due the RCMP's access and privacy coordinator for his personal commitment to reducing the number of well-founded complaints.

And National Archives continues to maintain its high standards—only four of 23 complaints were well-founded, three of which were resolved.

At the risk of appearing inconsistent, there is praise for Canada Post. Despite having the questionable honour of first place as the office's most important client, only 50 of the 230 complaints were well-founded. Of these, 37 were resolved.

	RESULTS				
GROUNDS	WELL-FOUNDED	WELL-FOUNDED RESOLVED	NOT WELL-FOUNDED	DISCONTINUED	TOTAL
ACCESS	30	70	320	16	436
Access	27	69	305	16	417
Correction/Notation	3	1	14	0	18
Index	0	0	1	0	1
Language	0	0	0	0	0
PRIVACY	17	45	141	16	219
Collection	0	11	22	3	36
Retention & Disposal	3	4	7	2	16
Use & Disclosure	14	30	112	11	167
TIME LIMITS	245	0	101	23	369
TOTAL	292	115	562	55	1,024

Although CSC seems to have conquered its delay problems, it had the worst ratio of justified complaints among the large institutions as 64 per cent—103 of 162—of the complaints investigated were considered well-founded. Not far behind were Employment and Immigration and Revenue Canada Taxation with 60 per cent and National Defence with 58 per cent well-founded.

Overall, investigators completed 1,008 investigations comprising 551 not well-founded, 402 well-founded and 55 discontinued.

This year the complaints have been grouped under three major headings. They are: access complaints—dealing with individuals' problems with their applications to see personal records; privacy complaints—concerning the fair information code (proper collection, use and disclosure); and time limits—including both delay in the initial response to an application or time extensions.

More resources please!

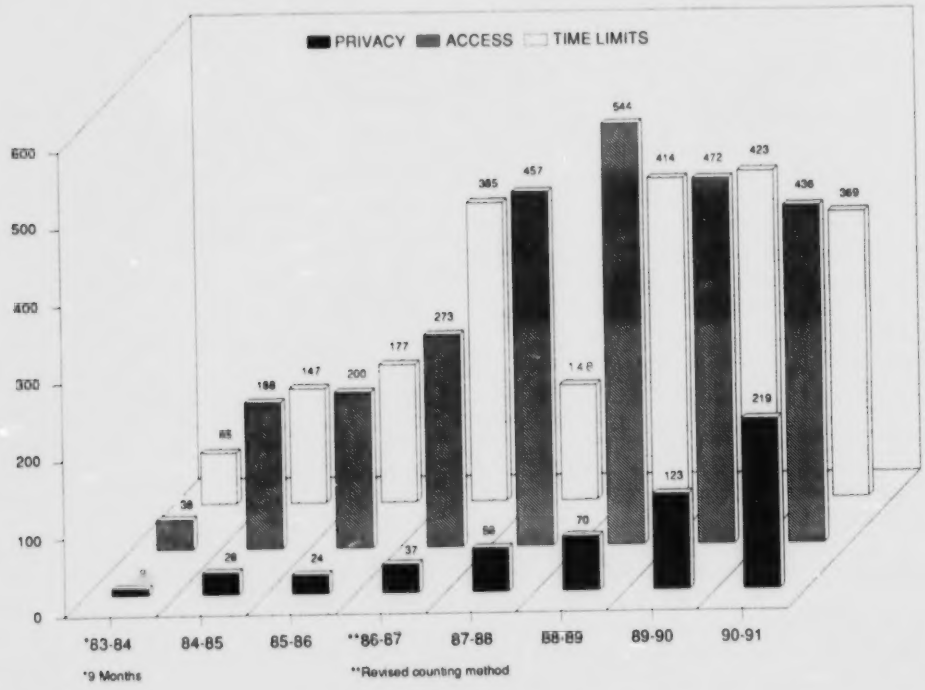
Despite having completed more than 1,000 cases, the norm for the past three years, 589 complaints were pending at the end of the year—a 38 per cent increase from the preceding year. Sadly, this means a return to the backlog the office worked so hard to eradicate two years ago. The problem will be compounded if the 10 per cent increase forecast for 1991-92 materializes—and it probably will if this year's 14 per cent increase is an indicator.

Unless the office receives more staff and money, its open caseload will soar to more than 700 complaints by the end of the current year. This represents more than the total caseload investigated by the office in the 1987-88 year.

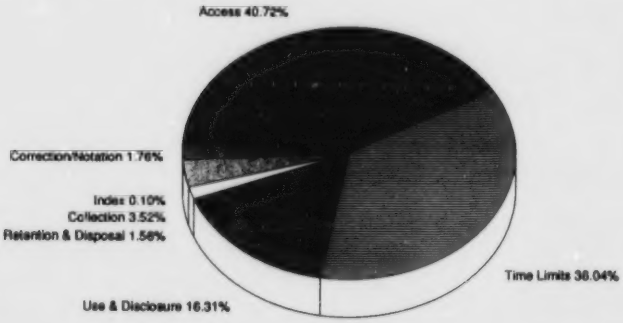
Despite increased productivity, the office has not closed more cases this year. Increased efficiency has been more than offset by the drop in time limit complaints (which consume fewer resources) and the rising tide of complaints against the fair information code (the most complex and time-consuming investigations).

Unfortunately the government turned down the office's request for more investigators and operating funds. This decision will exacerbate the ever-increasing backlog; increase investigator's caseloads and keep clients waiting longer for decisions on their complaints. In short, the office now risks becoming part of the problem.

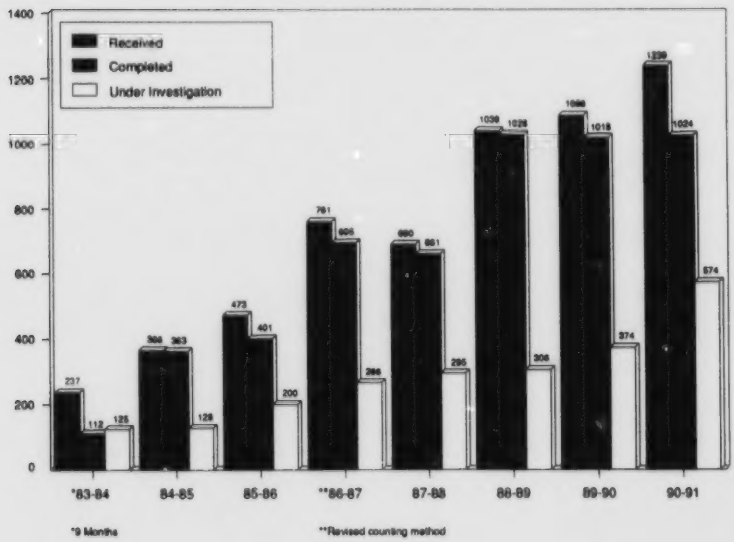
Completed Complaints and Grounds 1983-91



Complaints Completed by Grounds 1990-91



Completed Complaints 1983-91



Completed Complaints by Department and Result

Department	Results				
	Total	Well-founded	Well-founded; Resolved	Not Well-founded	Discontinued
Agriculture Canada	11	2	1	8	0
Canada Post Corporation	233	13	39	171	10
Canadian Human Rights Commission	5	1	3	1	0
Canadian Security Intelligence Service	83	6	9	67	1
Commissioner of Official Languages	1	0	0	1	0
Consumer and Corporate Affairs Canada	5	3	0	1	1
Correctional Service Canada	162	84	19	49	10
Employment and Immigration Canada	78	33	10	27	8
Environment Canada	1	0	0	1	0
External Affairs Canada	7	3	0	3	1
Farm Credit Corporation Canada	1	0	0	1	0
Finance Canada	1	0	0	1	0
Fisheries and Oceans	6	1	3	1	1
Health and Welfare Canada	34	16	3	15	0
Indian and Northern Affairs Canada	0	0	0	10	0
Justice Canada	9	2	0	7	0
Labour Canada	1	0	0	0	1
National Archives of Canada	24	1	3	19	1
National Defence	84	34	8	31	11

Department	Results				
	Total	Well-founded	Well-founded; Resolved	Not Well-founded	Discontinued
National Museums of Canada	1	0	0	1	0
National Parole Board	20	2	5	13	0
Privy Council Office	3	2	0	1	0
Public Service Commission of Canada	2	0	0	2	0
Public Service Staff Relations Board	7	0	3	4	0
Revenue Canada, Customs and Excise	14	11	1	2	0
Revenue Canada, Taxation	71	43	0	28	0
Royal Canadian Mint	1	0	1	0	0
Royal Canadian Mounted Police	78	2	3	66	7
RCMP Public Complaints Commission	1	0	0	1	0
Secretary of State of Canada	3	2	0	1	0
Solicitor General Canada	14	1	0	12	1
St. Lawrence Seaway	1	0	0	1	0
Statistics Canada	1	0	0	1	0
Supply and Services Canada	3	0	2	1	0
Transport Canada	42	27	2	12	1
Treasury Board of Canada	1	0	0	0	1
Veterans Affairs Canada	5	3	0	2	0
TOTAL	1,024	292	115	562	55

Origin of Completed Complaints

Newfoundland	0
Prince Edward Island	8
Nova Scotia	41
New Brunswick	38
Quebec	148
National Capital Region Quebec	3
National Capital Region Ontario	53
Ontario	457
Manitoba	66
Saskatchewan	33
Alberta	55
British Columbia	166
Northwest Territories	0
Yukon	5
Outside Canada	0
TOTAL	**1,024**

Cases

Tax files not for fan mail

A journalist got a fan letter from a federal employee at her home address and called the Commissioner's office to inquire how the admirer could have found her private residence. The journalist did not want to lodge a complaint or get the employee into trouble, but she was concerned both for her safety and how the information had been obtained.

The office was torn between respecting her wishes and ensuring that federal employees not use government files for purposes well outside the most generous interpretation of a "consistent use". The investigator tracked the source to Revenue Canada-Taxation.

Confronted with his letter, the employee explained that he simply wanted the woman's autograph. He did not appear to pose any threat to the journalist, who was relieved and asked that the case be discontinued.

However, the revelation that the employee used information from Taxation data obliged the office to tell Revenue Canada which has a strict code of ethics and imposes stringent security measures on handling taxpayers' files. Taxation investigated, found this was not the only incident and disciplined the employee.

Revenue Canada delays

Even though the *Privacy Act* has been in effect for eight years, failure to meet time limits continues to be a problem.

To name just one, Revenue Canada-Taxation occasionally displays an indifference to applicants' rights to receive their information within the time the law allows. Curious since Taxation promptly penalizes taxpayers who are casual with tax filing deadlines!

For example, on May 7, 1990, a woman went to the Vancouver taxation office to inquire about an application she had filed in January to see her income tax file. Taxation had no record of the request so she made another. On June 26, she called the Commissioner's office to complain that she had neither heard nor seen anything.

The office called Taxation to inquire. Even so, the woman did not receive the file until August 13, 96 days later. Departments are allowed to ask for a 30-day extension under some circumstances. However, they must notify the applicant who then may complain if she considers the extension unreasonable.

Revenue Canada had no justification for not writing to the woman to acknowledge her request, to say when it would provide the file and—ultimately—for not responding in time.

The Commissioner considered the complaint well-founded.

Court orders CSIS to respond

The Canadian Security Intelligence Service (CSIS) told an applicant that it could not provide the personal information he wanted in the 30 days the Act allows.

The delay was partly the result of many new applications (apparently prompted by an article in the **Toronto Star**) and by the need to consult other parties before it could release the material.

The man complained to the Commissioner and told the investigator that he intended to go to Federal Court if CSIS did not give him the information within the maximum 60 days set out in the Act.

On the 61st day, when the Commissioner found CSIS had still not finished processing the man's records, he concluded the complaint was well-founded and advised the complainant of his right to go to Federal Court. (Applicants may not ask for a court review until the Commissioner has completed his investigation.)

The complainant asked the court to issue a *Writ of Mandamus* which would compel CSIS to produce the information. The motion was heard 20 days later and the judge ordered CSIS to reply to the man's request within one month of the date of the order. CSIS complied.

Although CSIS finally provided the information, the hearing (and the extra month the court allowed) added yet another 50 days to the process — hardly a satisfactory solution. After eight years of living with the *Privacy Act*, it is unacceptable for applicants to have to go to court to force departments to provide timely access.

More access during military grievances

A complaint against National Defence (DND) may have prompted it to change its grievance procedures for military members. The case raised important questions about a member's access to factual information collected by DND's legal services during the grievance process.

At DND, lawyers may investigate military grievances to prepare legal opinions and advise the chief of defence staff. Normally, government staff relations officers (who are not lawyers) investigate such grievances. The military procedure effectively extends legal privilege over more of the documents.

The problem this causes became apparent when an officer complained to the Commissioner that DND had denied him a good deal of information from his grievance file, claiming exemptions for solicitor-client privilege or personal information about other individuals.

The investigator confirmed DND used the solicitor-client exemption on all the documents either obtained or prepared by its legal services during the grievance investigation. The department argued that the material became privileged since its legal services developed the file specifically to prepare a legal opinion and recommendations for senior staff.

The Commissioner was concerned about such a broad use of the solicitor - client privilege, considering it both unfair and contrary to the spirit of the act to use the privilege to withhold factual material and witness statements obtained during the investigation. He suggested DND use its discretion to disclose more information to the complainant. DND agreed to reconsider and gave the officer ten more pages of information including the witnesses' statements.

The Commissioner also agreed that the other disputed material was personal information about other individuals and that it was correctly exempted.

DND has since revised its military grievance procedures and now discloses to members all documents (with some limited exceptions) which the adjudicative authority will review when considering their grievances.

Can't claim exemption if doctor to disclose

A man complained to the Commissioner when National Archives denied him portions of his old military medical records, considering it to be not in his "best interest" (section 28) to examine a 25-year-old mental health assessment. National Archives was prepared, with his written consent, to give the information to his family doctor who could then explain the assessment.

Privacy regulations allow a department to require an applicant to examine personal health records only in the presence of a qualified medical practitioner or psychologist who can explain the information.

In this case, however, the man argued that he knew the contents of the assessment and did not need an explanation.

The Commissioner held that if Archives thought it was not in the applicant's best interest to see the records it should exempt them entirely. But if it intended to disclose them—even through his doctor—then it was inconsistent to claim it was not in his best interest.

The Commissioner was also concerned that Archives refused access based on a review by a psychiatrist retained to assess the file when the man submitted similar privacy requests in 1985 and 1990. The Commissioner considered the assessment unreliable since it was based solely on a review of medical files dating back 25 years and did not consider the man's current emotional state.

The information was disclosed after the Commissioner concluded that the man was entitled to see the file. Further, National Archives agreed to change its procedures for processing sensitive medical information. In future, it will either claim the medical exemption or disclose the information directly to the applicant or to his or her doctor.

Witness statements available after investigation

A woman who had lodged a discrimination complaint with the Canadian Human Rights Commission (CHRC) asked to see the information in the CHRC complaint file. She complained to the Privacy Commissioner when CHRC withheld some of the data.

What CHRC had refused to disclose was addresses and telephone numbers of other individuals and witness statements. The Commissioner agreed that others' personal information was legitimately exempt. However, he disagreed with exempting the witness statements once the investigation was completed.

Generally, the Privacy Commissioner agrees that witness statements should not be disclosed during investigations because this might harm the investigation. However, in the case at issue, the investigation was complete. The Commissioner asked CHRC to demonstrate what injury could reasonably be expected if the complainant saw the witness statements.

CHRC was unable to demonstrate any reasonable possibility that disclosure would injure either this or future investigations. Nonetheless, it took considerable persuasion before CHRC finally agreed to disclose the statements to the complainant. Since the information was initially denied, the Commissioner considered the complaint well-founded but resolved.

Revenue Canada can see personal expenses

An Ontario woman's difficulties paying her federal income tax arrears generated a complaint against Revenue Canada - Taxation. The woman was upset when an officer insisted on examining her personal expenses to assess her ability to pay. He maintained that the *Income Tax Act* gave him that right but the woman felt the procedure was abusive and an invasion of her privacy.

The *Privacy Act* limits government institutions' collection of personal information to that which "relates directly to an operating program or activity of the institution". This effectively restricts government collection to personal information which clearly is required for that program.

Revenue Canada explained that as administrators of the *Income Tax Act*, it is responsible for collecting individuals' income tax. The department has a collection procedure that ensures that the law is applied equitably to all taxpayers, but yet allows it to consider each individual's financial circumstances. In fairness to the majority who pay promptly, the department's policy deals firmly with those who do not.

The Commissioner reviewed Taxation's collection policy and agreed with the collection officer's need to examine the taxpayer's personal expenses. Under the circumstances the *Income Tax Act* requires her to provide this type of information. Thus, the Commissioner considered Taxation had respected the collection provisions of the *Privacy Act* and he concluded that the complaint was not well-founded.

Hiring must balance fairness and privacy

A complaint against Employment and Immigration Canada (EIC) demonstrated the difficulty of making the hiring process transparent without stripping away candidates' privacy.

Two successful candidates in an internal EIC competition complained that a staffing officer gave their personal evaluations and personal references to another employee who was appealing the results. This person then circulated the information in the office.

The Public Service Commission's policy on appeals requires departments to disclose only directly relevant personal information about the successful candidates. In this case the evaluations had been used during the staffing process but were neither referred to during the appeal nor considered as part of the appeal decision. Clearly they were not relevant. The disclosure was a significant invasion of the employees' privacy although the result of a perhaps overzealous attempt to be fair.

EIC reminded all its personnel divisions about the disclosure policy and will issue more detailed guidelines for staffing officers caught between the competing demands of fairness in staffing and protection of candidates' privacy.

Immigration disclosure of refugee claim "consistent"

A man wrote to the Commissioner objecting to an immigration officer having told officials of a U.S. state (without his consent) that he was claiming refugee status in Canada.

During his refugee hearing, it became apparent that the man had been found guilty of a criminal offence in a state but he had failed to appear for sentencing.

The complainant argued that since the process was not complete, his situation was not equivalent to a criminal conviction in Canada which would prevent him being considered a refugee. A senior immigration officer wrote to the clerk of the state's first circuit court to determine whether the man was considered to have been convicted. The letter explained that Immigration needed the information because the complainant had applied for refugee status.

The state court confirmed that the judicial finding of guilt was a conviction.

The investigator found that one of the objectives of the *Immigration Act* is "to promote international order and justice by denying the use of Canadian territory to persons who are likely to engage in criminal activity". The Commissioner concluded that revealing the man's refugee claim was permissible because it was consistent with Immigration's purpose for having obtained the information. He considered the complaint not well-founded.

Direct pay request premature

A Transport Canada employee complained that the department was asking for his bank account number so it could deposit his pay directly, rather than issue a cheque.

Transport's request apparently followed the federal government's announcement that it would stop paying employees by cheque on April 1, 1991 and begin depositing pay directly into employees' bank accounts.

The complainant objected strongly to having to give his bank account number to his employer. In fact, he was just one of a number who called or wrote to the office wanting to know if they had to provide the information.

The investigator identified two privacy issues. First, could Treasury Board (the employer) require employees to provide the location and number of their bank accounts for direct pay deposit? Did it have legal authority for collecting the information?

The Commissioner concluded that the government had the legal authority to decide how it will pay its employees. Collecting the necessary details to administer its pay procedure would not breach the *Privacy Act*.

However, the second issue concerned how the employer would deal with employees who refused to provide the information. Could it give their names, addresses and social insurance numbers to a bank to open accounts without their consent?

Privacy staff had several meetings with Treasury Board and were told that the program was still voluntary—Transport Canada had simply been eager to begin. No information had been collected except from those who had opted into the program. However, the Board acknowledged the problem of handling recalcitrant employees' pay.

Still, with the Minister's announcement in December 1989, it appeared that the public service was moving toward mandatory direct deposit. The Commissioner decided to hold the complaints open until the policy became clearer.

Then, on December 15, 1990, the government announced that direct deposit would remain voluntary. The complainants would not have to provide the information and the government would not be opening any accounts on employees' behalf. Thus, the Commissioner considered the complaint not well-founded.

Staff relations board exhibits now kept two years

Although privacy regulations require government agencies to hold personal information for at least two years, a complaint revealed that the Public Service Staff Relations Board (PSSRB) kept its exhibits for just three months before having them destroyed or returned to the party who presented them.

The two-year period was written into the regulations to give individuals enough time to examine the material if they were interested.

A woman complained that her privacy rights were infringed because the PSSRB destroyed the exhibits well before the two-year period.

PSSRB explained to the privacy investigator that it lacked the facilities to keep all exhibits—items ranging from volumes of documents to a broken baseball bat, garbage cans and even a hangman's noose! PSSRB staff also pointed out that all parties to a hearing receive copies of the exhibits so nothing was being destroyed that they had not already received.

Nevertheless, the regulations are clear. The Commissioner concluded that PSSRB must keep exhibits containing personal information for at least two years after taking the last administrative action. The Board agreed and the Commissioner considered the complaint resolved.

Personal information should be accurate

A veteran Canada Post employee complained to the Commissioner that the post office had given false medical information about him to the Workers' Compensation Board (WCB), in order to deny him benefits.

Canada Post had told WCB that the employee was ineligible because his injury was caused by a chronic medical condition. According to the employee's supervisor, the employee had given her the information and she was merely reporting what she thought might be relevant to the claim.

The employee denied having the condition and a recent examination by a specialist confirmed this. He also denied ever having told anyone, let alone his supervisor, that he had the condition.

During his inquiries, the investigator noted a factor which may have contributed to the problem. Canada Post manages the WCB claims aggressively in order to minimize costs. It argues that it is obliged to give WCB any information which could question the validity of the claim.

The *Privacy Act* requires that personal information being used for administrative purposes be as accurate, up-to-date and complete as possible. In this case there was no evidence that the supervisor had made any effort to verify that the medical information was accurate.

After protracted discussions. Canada Post agreed reluctantly to tell the WCB that it had no information to substantiate its allegation that the claimant had the medical condition.

The Commissioner considered the complaint well-founded and resolved.

Licence holders list not for surveys

An airline operator's call to the office about a Transport Canada drug use survey prompted the Commissioner to initiate a complaint of his own.

The caller became concerned when a market research company asked for the names, addresses and telephone numbers of his employees. The company said it was conducting a survey for Transport Canada on substance use in the transportation industry. It needed the personal information to randomly select participants for the survey.

The surveys, it was established, were a major component of Transport Canada's study to determine what risks employee use of drugs and alcohol posed to transportation safety in Canada. Participants were asked to complete a questionnaire about their use of alcohol, prescription, non-proscription and street drugs and about workplace conditions which could influence their using these substances.

Two areas of privacy concern surfaced:

- Was there an improper collection of personal information during the survey? and

- Did Transport Canada respect the use and disclosure provisions of the *Privacy Act*?

Controls on use and disclosure require government agencies to collect only personal information that relates directly to their operating programs or activities. The information must be collected directly from the individual (whenever possible) unless that would lead to collecting inaccurate information or defeat the purpose or prejudice its intended use. And the individual must be told why the information is being collected.

The investigation established that the questionnaires contained no identifying personal information to link them to any specific individual. Since the respondents could not be identified, the information was not personal and so its collection did not violate the *Privacy Act*.

However, it was clear that Transport Canada compiled the list of some survey participants from personal information it collected for other purposes, none of which included disclosing to research organizations. In most sectors Transport gave the survey company only the names and work telephone numbers. But, in the case of airport employees, its source was a list of employees licensed to operate airside vehicles and disclosing the names was not consistent with the original collection purpose and was improper.

The investigator also found that the survey companies began collecting the information before written contracts were in place. The draft contracts contained no references to the collection principles in the Act. As a result, representatives of Privacy, Supply and Services (the contracting authority) and Transport Canada met to ensure that all future contracts requiring personal information collection contain standard clauses about collection, retention, use, disclosure and disposal of information to ensure that they comply with the Act.

The Commissioner also recommended that Transport Canada obtain the individuals' consent before considering any future use of personal information that is not consistent with the original collection purpose.

Notifying the Commissioner

During the reporting year the office examined 50 notices from government agencies advising of their intention to release personal information "in the public interest" or to benefit an individual. The disclosures ranged from confirming citizenship so that individuals could receive pensions or awards to detailed reports on escapes from federal penitentiaries. In fact, inmate incidents have become a recurring feature of the notification process (see page 24 for greater detail).

The following are examples of other public interest notifications.

DND releases security clearance details

National Defence (DND) advised the Commissioner that it intended to give an employee normally exempt information from his security clearance file.

In the midst of processing the man's application to see his file, DND staff learned that provincial police had laid criminal charges against him, including one of sexually assaulting a former employee. His security file contained a military police interview with the plaintiff during which she detailed their longstanding sexual relationship. She had made it clear to the military police that it was mutually desired.

Since the *Privacy Act* allows investigative bodies (including military police) to protect sources interviewed during security clearance investigations, DND would normally have exempted the woman's comments. They concerned her as well as him and it would have been virtually impossible to extricate only the man's information from the record and the source of the comments would have been obvious. The department's dilemma was that it had accepted in confidence information which appeared to contradict the woman's charges. The man may not have known about the information in his file and therefore be deprived of details vital to his defence. DND concluded it was in the public interest to provide him the information before the matter went to trial.

The Commissioner notified the woman.

Woman given details on son's death abroad

A woman asked the RCMP and External Affairs to tell her what they knew about the death of her son in Thailand. Although both the RCMP and External had been satisfied with the Thai investigation, and a Canadian pathologist had confirmed the overseas postmortem results, the woman still had questions.

The RCMP intended to give her 21 pages from its inquiry report, exempting some limited information about other individuals. External, meanwhile, agreed to provide material from files located in two overseas embassies and Ottawa headquarters.

Normally the *Privacy Act* would protect the information—even from the man's mother. But both agencies considered it was in the public interest to give her the report so that she could pursue her inquiries in Thailand—and perhaps put her mind at rest. The Commissioner agreed.

List of unclaimed dividends sought

An applicant used the *Access to Information Act* to ask Consumer and Corporate Affairs for lists of unclaimed dividends under three acts: the *Bankruptcy Act*, the *Canada Business Corporations Act* and the *Winding-Up Act*. The applicant intended to track down the creditors.

CCA advised the Commissioner that it would release the lists because it would benefit the individuals concerned (paragraph 8(2)(m)(ii)). The Commissioner agreed but admitted to "lingering unease about the need for this disclosure", observing that if government institutions are reasonably able to locate individuals to whom they owe money, they should do so. He concluded that it "seemed less than ideal" to disclose personal information without consent to permit third parties to locate creditors (presumably for a fee).

Poor catch for Revenue Canada

Fisheries and Oceans advised the Commissioner that it intended to provide Revenue Canada's GST Communications Office with a mailing list of commercial fishermen. The GST office wanted to send fishermen an information booklet explaining how they should "charge, record, calculate and send in the tax". Revenue Canada had no other way of reaching fishermen and Fisheries concluded that clearly it was in the fishermens' interest to receive the material.

The Commissioner was not so sure. The GST legislation had not then been passed and, while it might be helpful, he was not convinced disclosure of the list would "clearly benefit" fishermen. However, he told Fisheries he had no objection to their mailing the material for Revenue Canada.

The Fisheries department could not find sufficient "public interest" to warrant its mailing GST material. It did, however, provide Revenue Canada with a list of fishermen's associations.

Board members' names not "personal"

The International Development Research Centre (IDRC) told the Commissioner it would release the names of board members who had attended an IDRC meeting in Bangkok, Thailand. The centre had given a journalist (who applied under the *Access to Information Act*) the members' expense accounts, but not the names. The journalist complained to the Information Commissioner who recommended release.

After discussing the notification with IDRC staff, the Privacy Commissioner agreed with the Information Commissioner that the board members were officers of the centre and so their expense accounts would not normally be "personal information". However, in preparing the initial package, IDRC had provided more detail than was necessary—-menu selections, insurance policy numbers, the credit cards they held and—in one case—the member's American Express Card number.

This level of detail went beyond the requirements of public accountability. Having made the mistake, IDRC could not then withhold the names. The Privacy Commissioner accepted the notification and IDRC advised its board members of the release.

Policy and Research

Data matching

Electronic data processing poses its own threats to privacy. For example, the uncontrolled linkage of computer files could produce extensive dossiers on everyone, making a mockery of the collection restrictions set out in the Act.

To guard against this, the government introduced a data matching policy requiring that departments submit detailed proposals to the Privacy Commissioner 60 days in advance of linking databases.The policy, little more than a year old, applies a brake to untrammelled data linkage by ensuring that this independent agent (the Privacy Commissioner) weighs the proposals against a set of approved criteria. The Commissioner also acts as an advocate for those who may be affected by the match.

However, some departments seem to view the Commissioner's role as something of a rubber stamp to be applied after a last minute phone call. But Treasury Board's policy is clear — and the Commissioner's assessment is serious. Notifying the Commissioner when the system is on the launchpad will only frustrate everyone and cause delays.

This year the Commissioner's staff examined 11 proposals resulting from this policy. Following is a brief description of each match and the office's conclusions. Anyone wishing greater detail on these — or guidance on formulating their own proposals — should call the office.

Matching Employment and Immigration Canada Adjustment Assistance records with Toronto welfare files

Federal, Ontario and Toronto officials formed a committee to grapple with some of the problems caused by the increasing number of refugee claimants on Metro Toronto welfare rolls.

One of the problems was determining whether a refugee is receiving financial support from Employment and Immigration Canada's Adjustment Assistance Program. The program provides refugees with funds until they have sufficient income to support themselves or for one year, whichever comes first. Refugees benefitting from this program are ineligible for welfare.

The committee was concerned that, without some type of verification, both programs could be subject to fraudulent claims. Members agreed that EIC and Metro Toronto should share data to prevent such occurrences.

At first, EIC considered the match a "consistent use" and offered the Commissioner little substantiation. However, after a good deal of consultation, EIC provided a rationale and set out the legislative base for data sharing.

The Commissioner was satisfied but asked EIC to follow Metro Toronto's lead and tell applicants that the government agencies would verify their eligibility. He further asked EIC to add a notice and consent statement to the application forms as well as to assess whether the match reduced fraud cases enough to justify the action. EIC agreed.

External Affairs INFONNEL project

Last year's annual report said External Affairs had asked that the office examine its proposed new personnel management system which would incorporate smaller data bases into a single system with more sophisticated processing capabilities. The system would allow management to forecast, track and record all personnel actions.

Privacy staff became concerned that the proposed degree of integration might well exceed Treasury Board's approved uses of this type of database and that the proposal did not provide enough detail on system security. The staff concluded that the system design did not meet the requirements of either the *Privacy Act* or the government security policy.

Follow-up documents and discussions have failed to resolve the difficulties. Thus the office's audit branch will examine the system.

Agriculture Canada's Security Information System.

Agriculture Canada consulted the office on its plan to transfer some personal employee data from its human resource system to a security information system. Agriculture came to the office early in the process with a proposal for a "cleansing match"– one which simply verifies or updates a data base. The proposal set out the rationale for considering the transfer a "consistent use" and acted quickly to amend the bank descriptions to reflect the changes. In this example, Agriculture respected the policy and the result was a painless and speedy review.

The Personal Locator Beacon Registry

The office gave its seal of approval to a new Department of Communications system containing data on owners of "personal locator beacons". The devices are small, portable transmitters which campers, canoeists and hikers carry and activate in an emergency. The beacon transmits a radio signal to facilitate search and rescue.

Communications proposed to set up a voluntary registry containing such data as owners' names, addresses, type of vehicle and activity (land, marine or air) and next of kin. The registry, available to National Defence and the RCMP, will also be linked to DND and Transport Canada's joint search and rescue information system.

The registry is entirely voluntary and limited to this specific purpose. Participants sign a consent form and are told of the disclosures. Finally, all personal data will be stored in a newly-created personal data bank and listed in the **Info Source** guide.

Managers' new career counselling service

The office also had no difficulties with a Public Service Commission proposal to create a registry for its new confidential counselling service to help improve managers' skills.

The service is voluntary and within PSC's mandate. Participants provide the information directly and are told how it will be used. PSC will set up a bank to contain the data.

GST and SIN

A Revenue Canada notification on data linkages required by the GST has not been so clean.

Early in 1990, the Revenue minister advised the Commissioner that the GST program would involve some data matching and would use the social insurance number to register individuals and sole proprietorships. The minister assured the Commissioner that Revenue Canada took its clients privacy very seriously and promised a detailed submission "within the next few months".

Now, the legislation has been passed, detailed regulations have been adopted on sharing information and the use of SIN and still the Commissioner awaits the promised "detailed submission". In fact, only late in 1990 has the department begun to consider the data matching implications. This office has pressed for details but without success.

Fishing licence and vehicle match withdrawn

Fisheries and Oceans abandoned a project to step up fishing regulation enforcement by matching fishing licence holders with fishing vehicle permits. Fisheries withdrew the proposal when it became apparent that there was no legal justification for the match.

Immigrants' health records match

Health and Welfare Canada submitted a proposal to assess immigrants' overall health by linking its Immigration Health Services Records with provincial medical records.

The department proposed to extract statistical data only and promised not to use it for administrative purposes.

Technically this type of match does not require the Commissioner's review but the office appreciated being advised. Health care matches are a sensitive area which continue to worry the Commissioner.

Correctional Services' information gathering

CSC advised the Commissioner's office of a proposal to improve its gathering of "critical information" on persons about to be admitted to the penitentiary population. The need for better information became apparent after two recently-released federal inmates committed murders in Toronto.

When an inmate arrives at a federal facility, CSC requests information from the police, courts and various correctional and parole authorities. Agencies often do not give these requests high priority and CSC is left without critical information on which to determine the inmate's proper security level or the possibilities for parole. The problem is most acute in Metro Toronto.

As a result, CSC proposed contracting with former Toronto police officers to coordinate assembling the information.

The office examined these contracts to ensure that clauses covered contractors' collection and use of the personal information, that the collection procedure itself complied with the *Privacy Act* and that any information collected would be stored in a bank and made available to the individuals. CSC had taken all of these concerns into account.

The office noted that such release to provincial agencies might require review by the Commissioner's provincial counterparts. The staff also recommended that federal provincial agreements be drafted to cover the exchanges.

CIDA overseas student inventory

The Commissioner's office continues to struggle with a Canadian International Development Agency (CIDA) project to establish an inventory of CIDA-funded students from overseas.

CIDA's own files are organized by project or country, making it difficult to retrieve individuals' names and addresses. To solve this, CIDA proposed a tracking system that would link Employment and Immigration student authorization files which contain the information CIDA wanted. To accomplish this, it intended to send an employee to search the EIC files.

Despite privacy staff cautions that no legal authority could be found for the exchange, CIDA submitted a formal proposal. During discussions with Employment and Immigration it became apparent that their staff knew little about the proposal and — like privacy staff — could find no legal basis for this linkage. They also did not intend to comply.

As a result, CIDA asked for more consultation time and since then has submitted two different proposals. Examining the match did, however, reveal an oddity — CIDA lists no personal data banks for students and trainees in the **Info Source** guide. This was brought to the attention of Treasury Board which is responsible for ensuring government agencies comply with the *Privacy Act*.

Offsetting debts against income tax refunds

Probably one of the longest-standing data matching assessments concerns the government use of SINs to identify persons who owe money and to deduct the amounts owed from income tax refunds.

In June 1990, the Office of the Comptroller General proposed a research project to assess the usefulness of such a program to recoup some of the $800 million owed to the Crown for overdue student loans. The office agreed to a research match but held that deductions from tax refunds should not begin without legislative amendments.

The office also wanted to be assured that money would not be deducted solely on the basis of "a hit"— simply appearing on both lists. A principle of data matching schemes requires that there be some independent verification before taking any administrative action.

These differences of opinion remained unresolved by February 1991 when the government tabled its budget. It did mention changes to allow government to recover money owing from tax refunds.

Apparently individuals will be given fair warning and special care will be taken to ensure that the deductions from refunds will not cause undue financial hardship.

Nevertheless the office maintains that this type of debt collection will require legislative amendment and not simply the mandate of the *Financial Administration Act* or claims that such behavior represents either "consistent use" of the information, or disclosure "in the public interest".

Technology Marches On

Employment and Immigration (EIC) is at the forefront of applying new systems technology to its workplace. This fact is not surprising considering the department serves about 3,000,000 UI clients, receives some 40,000,000 claimants' reports and handles 31,000,000 inquiries each year.

Smart Cards

EIC has briefed our office on a pilot project to use "smart cards" for unemployment insurance clients. The cards resemble most bank or credit cards but are really mini computers containing 64K memory—as powerful as some of the early personal computers. Clients applying for benefits would use the card to report periods of unemployment through publicly available machines. EIC mainframe computers would then determine the claimant's eligibility, calculate the benefits and credit the payment onto the card. The claimant could then use the card to withdraw cash from an automatic teller machine or make purchases through retail direct debit machines.

The pilot project is expected to begin in two locations in the fall of 1991.

There are two clear privacy issues: ensuring that the correct person is accessing the system; and safeguarding against matching the data with other unrelated personal information.

Access appears to be controlled. Clients enter the system using a personal identification number (PIN) which they have selected. There are highly sophisticated internal security safeguards which EIC believes cannot be compromised. EIC will watch system security closely during the pilot project and brief the Commissioner.

The second concern, protecting against data linkage, has also been taken care of. Internal safeguards will prevent the card from being used for any other transactions and bank and retail machines will be limited to receiving the funds for the transaction.

However, EIC sees the single card eventually being used for as many as eight different applications. For example, cards could link the holder to an electronic job-search database describing available jobs which match their training and experience. Or they could be used to verify and pay training allowances and place the holder on training programs.

With so many possible functions, the cards could be useful for other government agencies or even private companies. EIC could sell them unused space for data or financial transactions. However, EIC recognizes that multiple uses would require segregation of the functions to prevent merging or cross-over of the data from one program to another.

Much of this project is still in the conceptual stage. EIC estimates it will take three to four years to start the UI program, another three to four years to implement and a total of 10 years for multiple applications. The scope of this project may require amendments to EIC legislation. Our office has suggested that any changes should focus on protecting the card and the transaction process, rather than simply authorizing its use.

EIC's new telephone inquiry system

The Commissioner's office remains concerned about Employment and Immigration's Automated Voice Response Enquiry System (AVRES). This pilot project allows touch telephone users to get general unemployment insurance information or details about their own claim over the phone. Callers use the phone keypad to select options and identify themselves by entering their social insurance number and date of birth. The technology permits computers to answer thousands of routine calls.

The office learned about the system when a Quebec City radio station asked us whether this was a proper use of SIN. There is no doubt that EIC can use the SIN—it was devised for the UI program. However, our office was concerned that individuals' SINs and dates of birth are so widely available that using them for identification does not restrict access to that individual.

Recognizing the weakness of SIN and date of birth, EIC looked at other solutions—client waivers, system recognition of the client's phone number or a client-chosen personal identification number (PIN), similar to bank card numbers. Although PINs appear to be the best solution, this would require a year for development and the pilot project was on the verge of launching into Ontario. With mounting internal pressure, Treasury Board approval and the system about to go to tender, EIC decided to proceed.

The Commissioner conceded that EIC was best suited to decide how to use technology to serve the public. However, he urged the department to hold off until more secure protections were in place, observing that EIC was courting the risk of embarrassment and, possible improper disclosure of a client's information.

Alas, it was too late—the project had already expanded to London and Peterborough. EIC believes the expanded pilots will enhance development and perfect a new security gate for the national system.

Consulting the Commissioner

The Commissioner's Office always welcomes opportunities to exchange information with those interested in the progress of privacy protection. Often such inquiries are outside the office's scope so it acts as a privacy clearing house, assembling material or referring inquiries to other sources. For example, research staff handled requests from Australia's new federal privacy commissioner for background on Canadian medical research guidelines, the application of federal data matching policy to law enforcement, security and intelligence data and Canada's experience with covert surveillance.

The Commissioner received other requests from down under as well. Privacy committees asked for the Commissioner's general assessment of the *Privacy Act* and his office's experience. The Australian electoral commissioner wanted information on Canadian legislative protection of whistleblowers (there is none) and Telecom Australia was interested in Canada's handling of caller ID and call management phone services, as well as codes of conduct for telecommunications companies.

The Hong Kong Secretary for Home Affairs, researching data protection legislation, needed information on registering computer systems and licensing data banks. Both these controls are features of some strict European data protection schemes—particularly the British Data Protection Act. They are not part of any Canadian legislation so his inquiry was referred elsewhere.

The Commissioner's staff also provided provincial counterparts with background information on

- federal data matching experience (Ontario);
- the privacy implications of linking health care and socio-economic records (Quebec).

The staff also assembled the latest federal material on informatics applications of government databases and a management framework for disseminating corporate affairs databases. This was in response to a request from the Ontario Ministry of Consumer and Commercial Relations for information on the privacy implications of public data bases.

The Royal Commission on New Reproductive Technologies asked the Privacy Commissioner for input on the privacy implications of the new reproductive techniques. The Commissioner intends to make a submission once the genetics study is complete. In the meantime, he welcomed the consultations.

Inquiries

Inquiries to the office continue to climb. Inquiries officers handled 4,032 calls and letters, compared with 3,447 the previous year—an increase of 17 per cent.

Fifty-five per cent of the inquiries concerned the use of or interpretation of the Act. Here are some examples: Canada Post employees asked whether they had to sign a consent to release their medical records to the employer; inmates questioned whether penitentiaries could open their mail; and Transport Canada's privacy office wanted to know whether a person's voice (on an audio tape) is considered personal information. In each case, the inquirers were referred to Treasury Board or the Department of Justice for interpretation.

The second largest inquiry category—17 per cent—comprised calls about privacy problems outside the Commissioner's jurisdiction. Four per cent of these inquiries concerned federal agencies and Crown corporations not covered by the Act. In one instance, a correctional officer was upset because he was shown on a CBC telecast. Apparently the cameraman had assured him he was not filming but simply adjusting the lens. The man worried that appearing on camera could endanger his life and that of other guards who are sometimes threatened by inmates. Since CBC is not covered by the Act, the office could offer no help.

The other 13 per cent of these inquiries were about other levels of government or—frequently—the private sector. For example: A woman called to enquire about a job application given her by the Canadian Imperial Bank of Commerce (CIBC). The form asked for consent to disclose personal information from credit agencies and former employers and included a statement that "permission includes my consent to the release of personal information concerning me within the meaning of subsection 8(2) of the *Privacy Act*".

This puzzled the Commissioner's staff on two counts:

- the banks are not subject to the Act; and
- section 8 says that government may not disclose personal information without the individual's consent.

The subsection cited describes the exceptions to the rule, none of which could be remotely interpreted as including release to prospective employers!

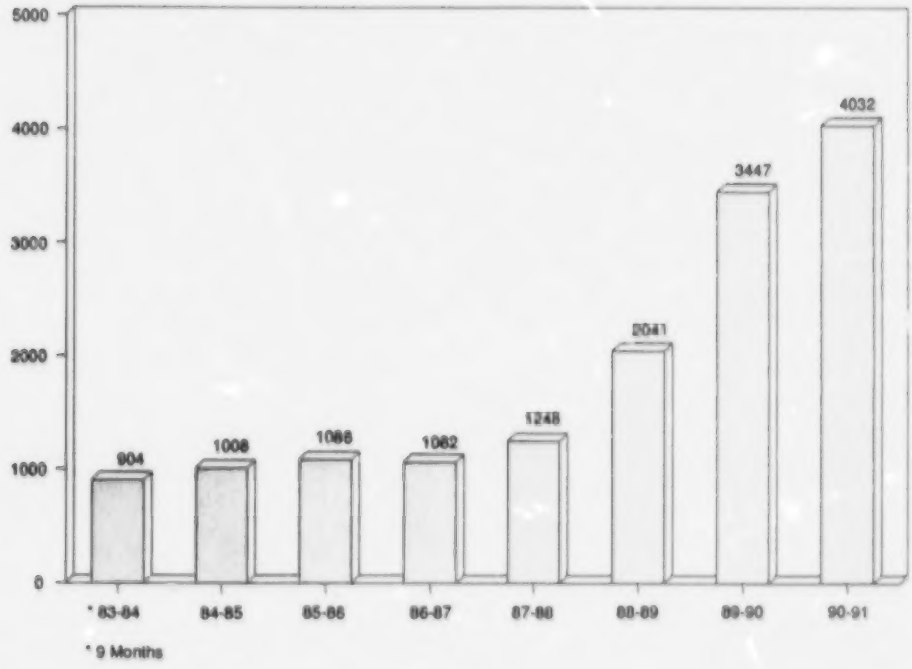
Staff concluded that the statement had no legal effect and did not dilute the protection of information held by the federal government. Legal counsels for both the office and CIBC discussed the consent, but, without jurisdiction, the Commissioner could not have the reference removed. And the bank has not apparently done so voluntarily since the office has received another complaint.

The most frequent Social Insurance Number (SIN) complaints (13 per cent of inquiries) cite insurance companies, video rental outlets, banks, grocery and department stores. Callers are amazed and unhappy that restrictions on uses of the SIN apply only to the federal government.

Several callers focused their anger on the Royal Bank's Gold Card application. The agreement requires applicants to consent to a blanket collection and disclosure of the SIN if they supplied it "in any application" to the bank. The office is inquiring whether opening a bank account (for which customers must supply a SIN under the Income Tax Act) is "an application".

Finally, eight per cent of inquiries were unrelated. A number of these deal with applying for a pardon and they are referred elsewhere. But many are from frustrated taxpayers who find in the office's toll-free line an opportunity to talk to a real person who works for "The Government".

Inquiries 1983-91



Compliance Directorate

The directorate's objectives for 1990-91 included auditing three major institutions, evaluating and improving the audit process and product, developing a privacy awareness component to audits and establishing an effective audit process for personal information held in electronic data processing (EDP) systems.

The office selected National Defence, the Royal Canadian Mounted Police and External Affairs, three institutions which hold the most sensitive and wide-ranging banks of personal information and operate some of the most sophisticated information handling systems in the country. While the war in the Persian Gulf and the Oka crisis at home had a serious impact on the success of the planned audit program, staff completed auditing the RCMP and DND and issued an interim report for External Affairs.

Due to the logistical problems and expense associated with international travel, the office has deferred its audit of External's overseas operation and the detailed review of its international information processing systems.

These agenda changes meant that the office could begin three smaller audits late in 1990; the National Capital Commission, the Office of the Comptroller General and the Commissioner of Official Languages. One of these, the Commissioner of Official Languages, was completed by year end.

The directorate now offers a "privacy awareness component" as part of its audits. Audit teams provide on-site presentations on the *Privacy Act* and have available two video cassettes which graphically illustrate the concerns pursued in the compliance audit. The videos are used only when the client institution chooses to become more informed.

All this year's investigations included an improved audit of information in computer systems. These new procedures and processes were used at DND, the RCMP and the Office of Comptroller General (OCG). In fact the OCG audit focussed entirely on EDP. Experience gained in these investigations will result in production of specific manuals and guides for this audit component.

The office was also involved in the following special investigations or projects:

- Cellular phone spectrum searching by the RCMP;
- CSIS establishment of an exempt bank;
- Indian Affairs and Northern Development (DIAND) internal audit;

- concerns about upward evaluation in Industry, Science & Technology and DIAND;

- the request for the release of Bell Canada technical information to the Criminal Intelligence Service of Ontario.

AUDIT FINDINGS

Royal Canadian Mounted Police

The audits to date have shown that the RCMP in particular has made a concerted effort to ensure that it complies with the *Privacy Act*. It has made privacy considerations a high priority, undertaking periodic information sessions at all levels and introducing training on the *Privacy Act* as part of the curriculum both for new recruits and officer trainees.

Although auditors found instances where personal information holdings were not adequately described in the Personal Information Index (now **Info Source**), these were due either to oversights or to descriptions not keeping pace with changes in operating procedures.

Some records containing personal information were not being disposed of in accordance with approved schedules and Privacy Regulations. This was particularly true with the disposal of performance logs (a type of manager's diary to record employees' daily performance). The logs were the subject of numerous meetings between privacy staff and RCMP privacy personnel, all seeking a solution that would satisfy both the privacy requirements and the force's administrative needs.

The audits found some instances of personal information not being adequately protected against unauthorized disclosure. The most serious involved the Victims Assistance Program where auditors found that volunteer counsellors have been given access to complete investigation files.

Two areas of particular interest examined during the RCMP audit were facsimile (FAX) transmission and using micro-computers to handle personal information. It is a pleasure to report that the RCMP has specific policies and procedures on transmitting personal information by FAX and handling it by micro-computer. These controls ensure that sensitive personal information is transmitted only through the RCMP's own secure communications facilities. Auditors inspected a number of computer systems and found evidence that the personal information they contained was properly protected.

National Defence (DND)

The office has reported its detailed findings to National Defence and is awaiting management's response. The practice is not to describe audit findings publicly until staff have had an opportunity to examine the department's comments and discuss any areas that may be in dispute.

Other audits

Other audits disclosed that retention and disposal standards are not always upheld or are inadequate. There was evidence that personnel files are not generally disposed of on time and some personal information banks have indefinite retention periods. Some third party information, which could be inadvertently disclosed, is found on personnel files. Sensitive and inappropriate information is often found on some personnel files and the need-to- know principle is not in place in most institutions. The security for personal information held by many institutions is inadequate, while descriptions for many information banks are inaccurate.

In fairness, however, most personnel expressed interest not only in the audit objectives but also in the proper application of the *Privacy Act* throughout their institutions. In a number of cases staff corrected problems before the privacy investigators left.

Among smaller institutions with fewer resources to spend on applying the Act, there tend to be greater opportunities for inappropriate handling of personal information. Policies and procedures tend to be out of date or absent and general knowledge of the Act is consistently lower than in the major departments. The security of personal information collected by these institutions is usually at risk.

So it is refreshing to report on a smaller institution which generally handles personal information in accordance with the *Privacy Act*.

Office of the Commissioner of Official Languages

Throughout the audit of the Office of the Commissioner of Official Languages it was evident that although most employees had only a cursory knowledge of the *Privacy Act*, all had a high degree of concern for the proper management of personal information. Auditors agreed that this concern reflected the provisions in the *Official Languages Act* dealing with the confidentiality of complaint investigations.

Yet, there were instances of personal information not being adequately protected against unauthorized disclosure and in one case, the computer system's security features had been rendered inadequate due to improper administration and protection of passwords.

Common findings

Overall, some of the most common observations in all audits were:

Inadequate protection of personal information

- Managers, supervisors and other employees are allowed to see personnel files for routine administrative purposes. Records staff have access to their own and each others' personnel file, allowing them to see sensitive personal information for which they have no "need-to-know". (e.g. - Personal History Forms, results of credit and reference checks, medical diagnosis, details of family members, designation of beneficiary, Canada Savings Bonds purchases, United Way contributions, etc.)

- Some files contained a limited amount of third-party personal information, usually when the subject's name is on a list with other employees, often including everyone's Social Insurance Numbers.

- Usually personal information handled by microcomputers is not adequately protected either by external security provisions (keyboard locks, hard disc protection, etc.) or internal protection (accounts, IDs, passwords, partitions, backup, etc.).

- File jackets tend to bear the particulars of an individual along with the caption of the file. This is especially pertinent where the file relates to investigations, complaints or special requests. For example, one personal file jacket included notations about a sexual harassment allegation, including the victim's name. The information was clearly visible to mail clerks or anyone who saw the file on a desk.

Improper disclosure of personal information

- Personnel records often contain documents that should have been purged from the file or retained on other files. Individuals' medical information and security-related material are found in up to 10 per cent of the records sampled.

Misuse of personal information

- Information properly collected for specific purposes is sometimes used for follow-on purposes (e.g. personal harassment files used for grievance and discrimination cases).

Improper retention and disposal

- Many banks have improper retention and disposal schedules and proper schedules are not being maintained.

Corporate Management

Corporate Management provides both the Information and Privacy Commissioners with financial, personnel, administrative, informatics and library services.

Finance

The Offices' total resources for the 1990-91 fiscal year were $6,372,000 and 78 person-years, an increase of $567,905 and three person-years over 1989-90. Personnel costs of $4,897,442 and professional and special services expenditures of $577,300 accounted for more than 87 per cent of the total. The remaining $852,060 covered all other expenses.

The following are the Offices' expenditures for the period April 1, 1990 to March 31, 1991*

	Information	Privacy	Corporate Management	Total
Salaries	1,685,327	1,856,590	652,525	4,194,442
Employee Benefit Plan Contributions	288,230	323,380	91,390	703,000
Transportation and Communication	38,141	114,167	123,309	275,617
Information	84,446	58,546	5,549	148,541
Professional and Special Services	411,801	130,150	35,349	577,300
Rentals	3,952	2,214	11,413	17,579
Purchased Repair and Maintenance	14,628	3,919	9,676	28,223
Utilities, Materials and Supplies	9,847	14,978	30,655	55,480
Acquisition of Machinery and Equipment	176,236	51,508	85,672	313,416
Other Payments	6,145	3,475	3,584	13,204
TOTAL	2,718,753	2,558,927	1,049,122	6,326,802

* Expenditure figures do not incorporate final year-end adjustments reflected in the Office's 1990-91 Public Accounts.

Personnel

An increase of three person-years and a change of both the Privacy and the Information Commissioners contributed to an active personnel program. There were 45 staffing actions, including outside recruitment, promotions, the hiring of term employees and some reclassifications.

Administration

New space was fitted-up for occupancy in the fall of 1990 and some progress was achieved in the records management area, particularly in the scheduling of administrative records.

Informatics

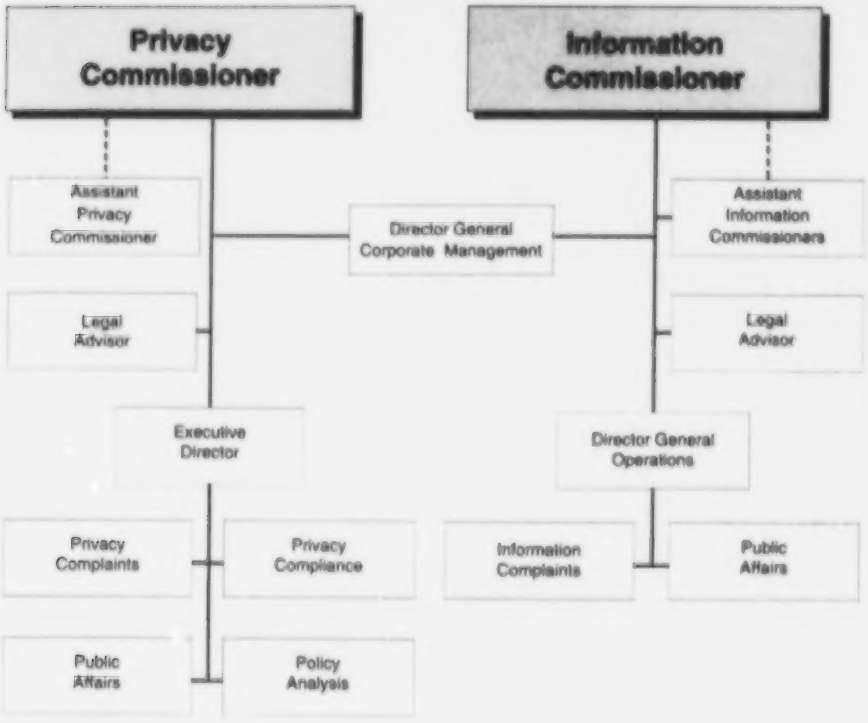
A new information technology was introduced to the organization. Three studies were undertaken concerning case management systems, additional office automation and networking in a secure environment. These studies will be completed in 1991-92 and will provide the necessary information to form a long-term information technology plan.

Library

The library provides services to the Information and the Privacy Commissioners. It is a resource centre for both the Information and Privacy staffs which is also open to the public.

A total of 436 books, periodicals, and annual reports were acquired through the Government Depository Services program. There were 835 items loaned and 847 reference questions answered. The automation of library functions was completed this year.

Organization Chart



Commissaire à la protection de la vie privée

Rapport annuel 1990-1991

Page 33 paragraphe 4

Le nombre de plaintes non fondées à l'endroit de la Gendarmerie royale du Canada devrait se lire 66 au lieu de 16. Le tableau que l'on retrouve aux pages 38 et 39 est exact.

Rapport annuel du Commissaire à la protection de la vie privée 1990-91

Le Commissaire à la protection de la vie privée du Canada
112, rue Kent
Ottawa (Ontario)
K1A 1H3

(613) 995-2410, 1-800-267-0441
Télec. (613) 995-1501

© Ministre des Approvisionnements et Services Canada 1991

N° de cat. IP30-1/1991

ISBN 0-662-58483-X

L'honorable Guy Charbonneau
Président
Sénat
Ottawa

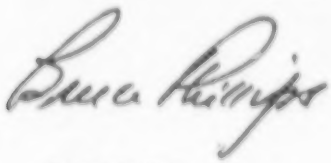
le 28 juin 1991

Monsieur Charbonneau,

J'ai l'honneur de soumettre mon rapport annuel au Parlement. Ce rapport couvre la période allant du 1er avril 1990 au 31 mars 1991.

Veuillez agréer l'expression de mes sentiments respectueux.

Le Commissaire à la protection de la vie privée



Bruce Phillips

L'honorable John A. Fraser, c.p., c.r., député
Président
Chambre des communes
Ottawa

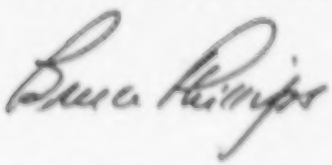
le 28 juin 1991

Monsieur Fraser,

J'ai l'honneur de soumettre mon rapport annuel au Parlement. Ce rapport couvre la période allant du 1er avril 1990 au 31 mars 1991.

Veuillez agréer l'expression de mes sentiments respectueux.

Le Commissaire à la protection de la vie privée



Bruce Phillips

Table des matières

Mandat 1

Le chef d'orchestre change, pas le refrain 2

La protection de la vie privée et la Charte 9

Les téléphones cellulaires et la protection de la vie privée 15

La protection de la vie privée dans le secteur privé 18

Tests biomédicaux 22

La réforme électorale - une liste électorale permanente 26

La protection de la vie privée et l'intérêt public: un équilibre difficile à protéger 28

Direction des plaintes 31
- Rapport de la Direction 31
- Tableaux et graphiques 35
- Dossiers 40
- Aviser le Commissaire 51
- Politique et recherche 55
  - Couplage de données 55
  - La technologie continue à progresser 62
  - Consultation auprès du Commissaire 65
- Demandes de renseignements 68

Direction de l'observation 70

Gestion intégrée 75

Organigramme 77

Mandat

La *Loi sur la protection des renseignements personnels* donne aux individus accès à leurs renseignements personnels détenus par le gouvernement fédéral; protège la vie privée des individus en restreignant le nombre des personnes qui peuvent consulter les renseignements; et donne aux individus un certain contrôle sur la collecte et l'usage des renseignements par le gouvernement.

La Loi énonce les principes des pratiques équitables en matière d'information qui exigent que le gouvernement:

- ne collecte que les renseignements dont il a besoin pour exécuter ses programmes;
- recueille les renseignements directement auprès de l'individu concerné, dans la mesure du possible;
- informe l'individu des fins auxquelles ils sont destinés;
- conserve les renseignements suffisamment longtemps pour en assurer l'accès aux individus; et
- veille « dans la mesure du possible » à ce que les renseignements personnels soient exacts et complets.

Toute personne présente au Canada peut déposer une plainte auprès du Commissaire à la protection de la vie privée si:

- elle s'est vu refuser une partie quelconque des renseignements;
- le droit de demander la correction de certains des renseignements contenus dans le fichier ou de les annoter leur est refusé;
- le ministère prend plus des 30 jours initiaux ou des 60 jours maximums pour fournir les renseignements;
- la description du contenu des fichiers de renseignements donnée dans le manuel *Info Source* est incorrecte à un quelconque égard;
- la liste donnée dans ce manuel pour chaque ministère ne décrit pas tous les usages qui sont faits des renseignements personnels;
- une institution recueille, conserve, utilise ou élimine des renseignements personnels d'une manière qui contrevient à la *Loi sur la protection des renseignements personnels*.

Les enquêteurs du Commissariat à la protection de la vie privéew examinent tous les fichiers (y compris ceux considérés inconsultables), à l'exception des renseignements confidentie's du Conseil privé de la Reine, pour s'assurer que les institutions fédérales se conforment à la Loi.

La Loi confère également au Commissaire à la protection de la vie privée le pouvoir de vérifier la façon dont les institutions fédérales recueillent, utilisent et éliminent les renseignements personnels, sans devoir attendre qu'une plainte soit déposée.

Le chef d'orchestre change, pas le refrain

Ce rapport annuel du Commissaire à la protection de la vie privée est le premier en huit ans à ne pas être soumis au Parlement par John Grace. Jusqu'en juin 1990, M. Grace a été le seul Commissaire à la protection de la vie privée que le Canada ait connu, depuis 1983, quand sa fonction est devenue distincte de celle du Commissaire aux droits de la personne.

M. Grace a quitté le Commissariat avec une réputation remarquable à de nombreux égards, d'abord parce qu'il a été un ombudsman doué d'un talent exceptionnel pour régler des problèmes et des plaintes en matière de vie privée, puis parce qu'il a su être un apôtre énergique et éloquent de la protection de la vie privée et enfin parce qu'il a été le chef respecté d'un petit groupe d'enquêteurs et de vérificateurs très motivés, auquel il a communiqué son engagement indéfectible pour ce secteur aussi vital que menacé des droits de la personne.

En outre, M. Grace a toujours été sensible aux défis qui continuent d'être jetés en si grand nombre - et à une vitesse vertigineuse - aux défenseurs de la vie privée, dans un environnement commercial et technologique toujours changeant.

Bref, John Grace a légué à son successeur une organisation bien rodée.

Une grande partie des questions qui figurent dans ce rapport annuel ont été abordées avant le départ de M. Grace.

Il s'est écoulé une dizaine de mois entre le départ de l'ancien Commissaire et la confirmation du nouveau. Pendant cette période, le directeur général, Alan Leadbeater, a assumé à titre intérimaire les fonctions de commissaire, en jouant un double rôle difficile, celui de directeur administratif et d'ombudsman.

Sous certains aspects, le nouveau Commissaire, qui est entré en fonction presque à la veille du dépôt du rapport, est le porte-parole de ses deux prédécesseurs, qui l'ont fait bénéficier de leurs conseils et de leur expérience pendant qu'il était commissaire adjoint. Les dix mois qu'il a passés à ce poste ont été pour lui une période inestimable d'introduction à un domaine dont la complexité déjà grande s'accroît sans cesse. Si le lecteur décèle un certain manque d'assurance dans le ton du rapport, il n'aura pas tort de l'imputer au fait que son auteur sait qu'il a encore beaucoup à apprendre.

Qu'à cela ne tienne, il n'est pas le seul! En effet, la relève de la garde s'est faite aussi au Québec et en Ontario cette année. Paul-André Comeau est devenu le nouveau Commissaire à l'information et à la protection de la vie privée du Québec, et Thomas Wright a assumé les mêmes fonctions en Ontario. Bref, les titulaires ont changé, mais la relation de cordialité et d'aide mutuelle des trois Commissariats, elle, devrait se maintenir sans difficulté.

Dans le rapport de cette année, tout comme dans ceux des années précédentes, nous tenterons de brosser un tableau réaliste de la situation de la protection de la vie privée au Canada, c'est-à-dire de donner et les bonnes, et les mauvaises nouvelles. Dans un domaine comme celui-là, la victoire n'est jamais acquise. En effet, la protection de la vie privée est si intimement liée à la relation entre l'individu et la société que l'évolution du tissu social se répercutera toujours sur la vie privée des citoyens.

Dans la société complexe d'aujourd'hui, rien n'est plus fragile, en dépit de toute son importance, que le droit de compter sur une intimité raisonnable. Contrairement à ce que certains cyniques prétendent, ce n'est pas un droit invoqué seulement par ceux qui ont quelque chose à cacher, car si nos libertés d'expression fondamentales ne sont pas protégées par un certain respect de notre intimité, il ne sera plus possible d'avoir des idées, des amis et des connaissances.

En 1898, lorsqu'il a donné une définition restée célèbre du droit à la vie privée (le droit qu'on nous laisse tranquille), le juge Brandeis n'aurait jamais imaginé un monde de machines ingénieuses dotées d'une capacité illimitée pour collecter, colliger et transmettre des renseignements dans des réseaux planétaires, pas plus d'ailleurs qu'une science capable de sonder les arcanes les plus secrètes de l'hérédité de l'être humain.

S'il a jamais existé, le droit qu'on nous laisse tranquille ne subsiste plus que dans les coins les plus reculés de l'Arctique, et encore... En effet, il y a gros à parier que nos ermites verront bientôt apparaître à l'horizon des fonctionnaires intrépides porteurs de la formule suprême qui, dûment remplie, leur conférera le certificat irréfutable d'appartenance à l'espèce humaine, un numéro d'assurance sociale.

Bref, dans notre société moderne, il est impossible de protéger complètement son intimité; ce n'est d'ailleurs ni pratique, ni même particulièrement désirable, mais nous continuerons à lutter pour préserver le droit de chacun de déterminer jusqu'à quel point sa vie privée doit être sacrifiée à d'autres droits.

C'est pour cette raison que l'idée d'un tableau annuel de la situation risque d'être trompeuse, si utile qu'elle soit pour évaluer les résultats, à moins que nous ne comprenions clairement qu'en matière de protection de la vie privée, les citoyens sont toujours en danger, étant donné qu'ils subiront immanquablement de nouvelles attaques dès qu'on aura trouvé la parade aux anciennes.

À la lecture des rapports annuels antérieurs, on ne manque pas d'être frappé par ce phénomène. Bien des questions qui dominent la discussion aujourd'hui faisaient à peine partie de notre lexique il y a tout juste huit ans. De nos jours, nous parlons énormément de dépistage des drogues et du SIDA, ainsi que des implications de la recherche juridique et de l'interception des communications par téléphone cellulaire, pour ne citer que quelques exemples, et nous reviendrons d'ailleurs sur certains d'entre eux plus loin. Il est certain que cette tendance se maintiendra, car rien ne laisse entrevoir le moindre ralentissement du progrès des sciences et de la technologie. Le mieux que nous puissions faire, c'est monter la garde pour être prêts à endiguer les attaques contre la vie privée, en tentant de réparer les brèches au fur et à mesure et en n'étant sûrs de rien, sauf que la lutte se poursuivra indéfiniment.

Cela dit, comment les choses se sont-elles passées au cours de la dernière année?

Eh bien, rien ne nous permet de croire que la vague technologique qui sape notre intimité soit en voie de s'apaiser. Les ordinateurs continuent à proliférer (l'administration fédérale à elle seule en aurait 80 000, selon les dernières estimations); le courrier non sollicité continue à s'accumuler; le commerce des renseignements personnels prend de plus en plus d'ampleur (son chiffre d'affaires annuel atteint les 3 milliards de dollars aux États-Unis, ce qui correspond probablement à 300 millions de dollars au Canada).

Et pourtant, si nous partons du principe que la vie privée ne peut avoir de meilleur défenseur qu'un public bien informé et désireux d'agir, l'année écoulée laisse entrevoir des indices très encourageants de gains réels et durables.

Dans le secteur privé

Les rapports annuels antérieurs ont fait état d'une sensibilisation croissante du public aux méthodes de marketing invasives du secteur privé. En 1990, cette question a même reçu la suprême accolade médiatique, la Une du TIME. En outre, et même si certains des participants auraient peut-être voulu échapper à cette publicité, une autre preuve de l'importance accrue que l'opinion publique accorde à la protection de la vie privée nous est venue de l'arène politique dans deux provinces où des ministres ont éprouvé de telles difficultés par suite de divulgations de renseignements personnels que l'un d'eux a dû démissionner. Quoi qu'on puisse en penser, ces événements montrent bien qu'on ne peut pas toujours faire fi impunément du droit à la vie privée. En fait, si le marché a été ces dernières années la source de certaines des pires menaces pour notre intimité, il se peut fort bien qu'il finisse par s'autocorriger, au moins en partie dans son propre intérêt.

C'est sans doute en réponse à une inquiétude croissance des consommateurs que le secteur privé semble commencer à prendre des mesures encourageantes. Certains diront sûrement qu'il est plus que temps, mais il reste que l'Association des banquiers canadiens, Bell Canada et l'Association canadienne du marketing direct se sont donné l'an dernier des codes d'éthique qui amélioreront sensiblement la protection des renseignements personnels et confidentiels concernant leurs clients. Nous vous en parlerons davantage plus loin, mais il vaut la peine de préciser dès maintenant que ces mesures d'autoréglementation ont des possibilités.

En fait, il ne s'agit pas tant de savoir si le secteur privé peut continuer à se passer de codes de protection des renseignements personnels, mais plutôt combien de temps il pourra le faire avant qu'on lui impose des règles. Les événements récemment survenus en Europe empêcheront peut-être bientôt les entreprises nord-américaines de se livrer à des transferts de données avec leurs homologues européennes à moins d'avoir des codes de ce genre. Cette évolution rend plus urgente encore la recommandation que le Commissaire avait adressée au Parlement l'an dernier, en demandant que la *Loi sur la protection des renseignements personnels* soit modifiée de façon à obliger toutes les entreprises privées de compétence fédérale à adopter des codes de protection des renseignements personnels fondés sur des règles et des principes internationalement reconnus.

Cela dit, même si les codes d'autoréglementation deviennent chose courante sur le marché canadien, seront-ils vraiment efficaces? Des spécialistes très respectés restent convaincus qu'un contrôle s'impose avant que l'entreprise privée soit en mesure de rendre des comptes au public sur ses activités de protection de la vie privée.

Le professeur David Flaherty, l'universitaire canadien le plus réputé en matière de recherche sur la protection de la vie privée, soutient que l'administration fédérale doit pouvoir faire des vérifications pour que le secteur privé respecte ses propres codes d'autoréglementation. Son opinion pèse lourd dans la balance, mais le Commissaire continue à croire, à l'instar de son prédécesseur, qu'une intervention d'une telle ampleur - avec les ressources énormes qu'elle nécessiterait - ne devrait avoir lieu qu'en dernier recours, si l'on prouve hors de tout doute que le secteur privé ne peut pas ou ne veut pas s'autoréglementer.

Il reste manifestement bien du chemin à faire jusque là. Nous ne citerons qu'un petit exemple : dans leurs demandes de cartes de crédit, certaines banques à charte réclament encore - en petits caractères - une renonciation de leurs clients à tous leurs droits à la vie privée. Ces renonciations donnent aux banques le droit de réutiliser à leur gré tout ou partie des renseignements que leurs clients leur fournissent, notamment sur leur traitement ou leur salaire, leurs antécédents professionnels et leurs biens, ainsi que, dans un cas, leur numéro d'assurance sociale. Quelques consommateurs alertes ont remarqué

les renonciations qu'on leur demandait de signer et ils en ont informé le Commissariat, mais nous craignons que la plupart n'y aient vu que du feu. Des dispositions contractuelles comme celles-là, imprimées en petits caractères, ne satisfont absolument pas aux exigences d'obtention d'un consentement en toute connaissance de cause. Qui plus est, elles ne reflètent pas l'attitude de respect accru de la vie privée dont l'Association des banques à charte se réclame désormais.

Cela dit, il y a eu des progrès. Nous devons notamment féliciter l'Association canadienne du marketing direct, qui a adopté une méthode grâce à laquelle les consommateurs peuvent faire rayer leur nom des listes d'expédition de leurs membres.

C'est un pas en avant, parce que l'Association regroupe environ 80 p. 100 des entreprises faisant du marketing direct.

Il reste que des améliorations aussi modestes sont bien insuffisantes face à l'explosion du volume des échanges de renseignements rendus possibles par l'ordinateur. C'est pourquoi le strict minimum en matière de normalisation des échanges de renseignements personnels doit être l'introduction de codes dûment approuvés de protection de ces renseignements pour toutes les entreprises de compétence fédérale. Pour le Commissaire, c'est urgent.

Nous recommandons aussi au Parlement de prendre des mesures pour rétablir la protection des communications téléphoniques personnelles au Canada, qui tend à s'éroder en raison de la prolifération des téléphones cellulaires. En effet, ces communications électroniques risquent d'être aisément interceptées par de l'équipement qu'on peut se procurer facilement, et elles le sont effectivement. L'absence de fils téléphoniques ordinaires ne devrait pas priver les usagers du téléphone du droit à leur vie privée et du droit de s'attendre à ce que leur intimité soit protégée. La vente ou la possession d'équipement de surveillance devrait être interdite, sauf dans le cas des organismes autorisés à s'en servir conformément à la législation qui régit ce genre d'activités.

Évaluation des gestionnaires

Les lecteurs du rapport annuel de l'an dernier se rappellent peut-être avec quelle froideur le Commissaire avait accueilli l'idée d'une ligne ouverte que les fonctionnaires auraient pu utiliser pour dénoncer la fraude, le gaspillage et la maladministration dans les institutions fédérales, sous le couvert de l'anonymat. Heureusement, l'idée a été abandonnée.

Néanmoins, le nouvel outil de gestion que les ministères et organismes adoptent avec enthousiasme, l'évaluation inversée (ou si l'on préfère de bas en haut) présente une grande partie des mêmes dangers pour notre vie privée. Comme le terme l'implique, c'est un procédé qui permet aux subalternes d'évaluer - anonymement - le rendement de leurs supérieurs. Jusqu'à présent, il a été utilisé dans de grandes entreprises privées, mais il est tout nouveau pour les institutions gouvernementales, qui refondent actuellement leurs systèmes d'évaluation du rendement dans le contexte de la réforme globale de la fonction publique.

Pour ce genre d'évaluation, le subalterne remplit un questionnaire en cotant son supérieur en fonction de ses aptitudes de gestion et de ses traits personnels. Les questionnaires remplis sont ensuite analysés, parfois par un contractuel, et leur contenu est résumé. Les cadres reçoivent un exemplaire du rapport qui en résulte, mais ils n'ont pas accès aux cotes ou aux commentaires de leurs subordonnés.

Le procédé soulève plusieurs difficultés en matière de protection de la vie privée, la première étant, bien entendu, le fait qu'on promet aux «évaluateurs» que les renseignements fournis seront traités de façon confidentielle pour leur éviter des représailles. En effet, *la Loi sur la protection des renseignements personnels* donne à chacun le droit de savoir ce qu'on dit ou ce qu'on écrit à son sujet. Par conséquent, si l'on promet à ceux qui font les évaluations que celles-ci seront traitées de façon confidentielle, on les induit en erreur, car cette promesse est illégale.

Par contre, il est bien établi dans la fonction publique que des subordonnés consultent, commentent et même contestent, s'ils le désirent, les évaluations de leur rendement faites par leurs supérieurs.

Cela dit, il est dangereux et tout à fait injustifié de prétendre qu'on peut contourner le droit à la vie privée en confiant ces évaluations inversées à des contractuels. Si c'était possible, l'administration fédérale pourrait se soustraire à tous ses objectifs de protection de la vie privée en confiant toute la gestion des renseignements personnels à l'entreprise privée. Les risques sont énormes et vont bien au-delà de ce que les cadres risqueraient s'ils perdaient leur droit d'accès à l'information qui les concerne et du fait que la Loi ne protégerait plus des renseignements aussi personnels d'une utilisation ou d'une divulgation abusives. Il reste que, une fois le marché conclu, les contractuels sont des agents de l'administration fédérale, et que celle-ci conserve donc le «contrôle» des renseignements en question où qu'ils soient conservés.

Bien peu de gens contestent le désir du gouvernement d'améliorer la gestion et l'imputabilité de l'administration fédérale, mais il fait sûrement fausse route en choisissant pour le faire un procédé qui saperait sa propre législation.

L'année du Commissariat

Comme presque chaque année depuis la création du Commissariat, le nombre de plaintes, d'enquêtes et de vérifications a augmenté. Les détails sont présentés dans d'autres chapitres du rapport, mais un fait demeure: le Commissariat fonctionne à plein rendement, et, nonobstant les restrictions globales d'aujourd'hui, les députés et sénateurs doivent bien se rendre compte que les obligations qu'ils lui ont imposées aux fins de l'application de la *Loi sur la protection des renseignements personnels* ne peuvent continuer d'être assumées de façon efficiente qu'au prix d'une modeste augmentation de l'effectif actuel de 34 personnes. En effet, nous traitons aujourd'hui plus de 1200 plaintes par année, soit plus de 160 par enquêteur. L'expérience nous a appris que nous n'échapperons pas à une importante augmentation de cette charge de travail, mais cette augmentation nous forcera à réduire la qualité du service.

La Direction de l'observation a aussi été très occupée. Il faut toutefois souligner qu'en huit ans d'activité, elle n'a pu faire des vérifications que dans environ le cinquième des 150 ministères et organismes fédéraux assujettis à la *Loi sur la protection des renseignements personnels*. Il est donc bien évident que, si l'on veut élargir la portée de la Loi et charger la Direction de faire des vérifications dans le secteur privé, son effectif de neuf personnes ne suffira pas à la tâche.

Dans le domaine de la recherche, le Commissariat a concentré ses efforts de la dernière année sur une étude des implications du dépistage des drogues en matière de protection de la vie privée. Ses travaux l'ont amené à conclure que les tests de dépistage obligatoire au hasard administrés par l'employeur sont injustifiés, voire, dans certaines circonstances, probablement illégaux. Le Commissariat a été heureux de constater que Transports Canada a modifié dans une certaine mesure ses projets de dépistage des drogues, mais il est très déçu de voir que le ministère de la Défense nationale et au moins une banque à charte vont adopter des programmes de dépistage qui constituent des violations injustifiées de la vie privée de leur personnel. (Cette question est analysée de façon plus détaillée dans un autre chapitre du rapport.)

Enfin, nous mettons la dernière main à un rapport sur les répercussions des progrès de la recherche et du dépistage génétique, qui constitue de toute évidence une plus grande menace pour la vie privée que le dépistage des drogues. Ce rapport devrait être publié à la fin de l'été 1991.

La protection de la vie privée et la Charte

Pour le Commissaire à la protection de la vie privée, il est à la fois fascinant et encourageant de voir la Cour suprême du Canada accorder une si grande place au droit à la vie privée dans le contexte de la *Charte canadienne des droits et libertés*. C'est fascinant, puisqu'il y a des hauts et des bas, et encourageant aussi parce que, dans l'ensemble, le droit à la vie privée se renforce.

Il a déjà été question de ce dossier passionnant dans deux rapports annuels antérieurs. Cette année, il y a plus encore à dire.

Le 11 septembre 1983, la police avait saisi 278 livres de marijuana dans un véhicule et accusé plusieurs personnes de conspiration en vue de l'importation d'une substance illégale. L'accusation était fondée sur les enregistrements de 136 appels téléphoniques interceptés au cours d'une enquête poussée dans des localités de la Colombie-Britannique très éloignées les unes des autres.

La police croyait que les complices communiquaient en utilisant des téléphones publics payants. Elle avait donc installé des dispositifs d'écoute sur vingt de ces téléphones, qui avaient été reliés à des enregistreuses à quelque vingt reprises, pour enregistrer automatiquement, la nuit durant, les conversations téléphoniques des suspects et d'autres personnes. La police avait bien sûr obtenu des autorisations judiciaires pour installer des appareils d'écoute sur des téléphones, mais jamais expressément sur des téléphones publics. Plus exactement, les autorisations comportaient une clause générale permettant à la police d'intercepter des communications à certaines adresses et "...à d'autres endroits de la Colombie-Britannique fréquentés par (les suspects)..."

Le juge de première instance avait conclu que les autorisations judiciaires étaient invalides, car, à moins d'avoir été expressément autorisé par un juge, l'enregistrement automatique des conversations faites à des téléphones publics payants équivaut à du ratissage, ce que le *Code criminel* ne permet pas. Le juge avait donc considéré les communications interceptées comme inadmissibles en preuve et il avait enjoint au jury d'acquitter les accusés.

La Cour d'appel de la Colombie-Britannique n'avait pas été du même avis; elle avait renversé la décision rendue en première instance et ordonné la tenue d'un nouveau procès. Dans sa conclusion, elle avait déclaré qu'il n'était pas nécessaire que l'autorisation fasse expressément mention de téléphones payants, pourvu que la surveillance de ces téléphones n'ait pas été systématique. Pour la Cour d'appel, la communication interceptée en elle-même pouvait prouver que la surveillance téléphonique n'avait pas été systématique, du moment qu'on pouvait y entendre la voix d'un suspect.

La Cour suprême du Canada a tranché la question à la majorité (à quatre contre deux), dans *Thompson et autres* c. *La Reine*. Cet arrêt rendu public le 18 octobre 1990 est extrêmement intéressant, mais plutôt curieux.

Dans les motifs de jugement de la majorité, le juge Sopinka a conclu que la clause générale d'autorisation était légale, même si elle ne faisait aucune mention des téléphones publics et ne prévoyait rien pour la protection du public. Toutefois, il s'est demandé si les interceptions « dûment autorisées » étaient « raisonnables », conformément à l'article 8 de la *Charte*.

Le juge Sopinka a conclu que, dans au moins quatre cas, on avait placé des dispositifs d'interception sur des téléphones publics simplement parce que ceux-ci étaient situés près de l'endroit où demeurait l'un des suspects. Selon lui, ce n'était pas là une preuve suffisante pour agir, car elle n'équivalait « ... à rien de plus qu'une surveillance systématique fondée sur une intuition » (p. 27). En outre, comme l'écoute risquait de porter atteinte à la vie privée de personnes innocentes (des centaines de conversations privées auxquelles aucun des suspects ne participait ont pu être interceptées), le juge a conclu que la surveillance constituait une infraction à l'article 8 de la *Charte*.

Venons-en maintenant à l'aspect curieux de cet arrêt. Le juge Sopinka a déclaré que l'utilisation de la preuve obtenue grâce à la surveillance électronique de téléphones publics ne risquait pas de discréditer l'administration de la justice. Il a donc rejeté l'appel et ordonné la tenue d'un nouveau procès.

Qu'y a-t-il de réconfortant à cela? La Cour suprême fait une mise en garde explicite contre les clauses générales autorisant l'utilisation de dispositifs d'écoute. Elle recommande fortement aux juges et à la police de réduire au minimum les risques d'intrusion dans la vie privée des personnes innocentes lorsqu'il est question d'autoriser l'utilisation de dispositifs d'écoute ou d'obtenir une telle autorisation et d'intercepter des communications. Et pourtant, la police se fait somme toute dire que, même si elle ne respecte pas les normes, elle pourra se servir de ce qu'elle aura découvert contre les suspects.

Les opinions dissidentes de M. le juge La Forest et de M^me^ la juge Wilson font ressortir les lacunes de l'opinion de la majorité. Les deux ont en effet déclaré que, puisque la surveillance électronique des téléphones publics donne lieu, par sa nature même, à d'importantes violations de la vie privée, les autorisations judiciaires requises doivent être expresses et non implicites, comme dans le cas de la clause générale des «endroits fréquentés». Faute de se prononcer en ce sens, la Cour suprême a laissé au Parlement le soin de s'assurer que la police ne violera pas la *Charte*. Ainsi, les rôles respectifs de la *Charte* et du Parlement ont été inversés. Le juge La Forest l'a déclaré avec éloquence:

> Il est évident que la Loi (*Code criminel*) et la *Charte* imposent aux tribunaux une lourde obligation de protéger la vie privée des Canadiens. La surveillance électronique est systématiquement acquisitive: sa portée vise les conversations tant des innocents que des coupables. La nature systématiquement acquisitive de la surveillance électronique incite les tribunaux à redoubler de vigilance et à être particulièrement conscients des risques que certaines pratiques minent l'attente des Canadiens en matière d'inviolabilité de leurs communications privées. Cette attente légitime et raisonnable en matière de vie privée ne survivra pas longtemps si les tribunaux accordent leur *imprimatur* à des pratiques qui permettent aux policiers d'intercepter des communications privées pour la seule raison qu'ils ont des motifs raisonnables de croire que de précieux éléments de preuve peuvent ainsi être obtenus. À mon avis, les clauses des «endroits fréquentés» peuvent facilement entraîner l'application de cette norme peu élevée et constituent des «recherches à l'aveuglette très étendues» dénoncées par notre Cour dans l'arrêt *Hunter* c. *Southam*, précité à la p. 167. Il est triste de penser que, même avec l'aide de la *Charte*, les tribunaux n'ont pas pris les mesures nécessaires pour prévenir ce danger et que si les Canadiens doivent être protégés adéquatement contre la menace insidieuse que la surveillance électronique pose à la vie privée, ils doivent se tourner vers le Parlement pour obtenir des garanties supplémentaires. Il y a une ironie cinglante dans tout cela. La *Charte* est destinée à nous protéger contre toute possibilité d'empiétement par le Parlement sur les droits individuels. (p. 14)

Par conséquent, l'arrêt *Thompson* ne peut guère inspirer au Commissaire que des sentiments mitigés. Nous devons applaudir quand la Cour suprême insiste - et c'est nouveau - pour que le droit à la vie privée des innocents soit protégé lorsque la police intercepte des communications privées. En outre, la Cour invite clairement les juges et la police à faire preuve d'une extrême prudence dans les cas où des dispositifs d'écoute sont installés dans des endroits fréquentés par le public. Bien que la Cour n'en fasse pas une obligation, elle recommande en outre que l'écoute électronique soit doublée d'une surveillance visuelle, pour faire en sorte que seules les conversations des suspects soient interceptées. Les Canadiens devraient être réconfortés de constater que la Cour suprême est consciente des risques que la vie privée

des innocents court lorsque la police utilise des dispositifs d'écoute électronique. Néanmoins, la Cour a aussi déclaré clairement que, pour que les Canadiens puissent être bien protégés contre des abus de ce genre, le Parlement doit renforcer les dispositions du *Code criminel* sur l'écoute électronique.

Le Commissaire à la protection de la vie privée se voit donc forcé de presser le gouvernement de proposer - et le Parlement de promulguer - les mesures nécessaires pour assurer un contrôle adéquat des pratiques de surveillance électronique.

Cela dit, la fiche de protection de la «vie privée» de la Cour suprême ne finit pas cette année en queue de poisson, tout au contraire : elle se termine par un coup d'éclat, avec la décision rendue dans *Santiago Wong* c. *La Reine* (22 novembre 1990).

L'arrêt *Wong* est le point d'aboutissement d'une enquête sur une maison de jeu menée par la police de Toronto à l'été de 1984. Les responsables de la sécurité d'un important hôtel du centre de Toronto avaient informé la police qu'ils soupçonnaient que des clients tenaient une maison de jeu à l'hôtel. On avait trouvé des indices dans une chambre d'hôtel qu'un client venait de libérer; la police avait appris que la personne qui avait réservé cette chambre, M. Wong, l'avait aussi réservée pour un autre jour, le même mois.

La police avait donc décidé d'installer une caméra vidéo dans la chambre, avec la permission de la direction de l'hôtel, mais sans autorisation judiciaire ni mandat. Les activités qui se sont ensuite déroulées dans la chambre ont été surveillées en cinq occasions, par suite de quoi M. Wong et dix autres personnes ont été accusés d'avoir tenu une maison de jeu.

Le juge de première instance avait conclu que la surveillance magnétoscopique était une violation de l'article 8 de la *Charte*, et il avait rejeté toutes les accusations. La Cour d'appel de l'Ontario avait toutefois jugé que les invitations à se rendre dans la chambre avaient été largement diffusées dans la communauté chinoise de Toronto, et que l'occupant de la chambre y avait reçu de purs inconnus. Compte tenu de ces faits, la Cour d'appel avait conclu que l'accusé ne pouvait pas raisonnablement s'attendre à ce qu'on respecte sa vie privée et que, par conséquent, l'article 8 de la *Charte* ne s'appliquait pas en l'espèce. Elle avait ordonné la tenue d'un nouveau procès.

En appel, la Cour suprême a tranché la question à six contre un en adoptant une autre position. La Cour concluait qu'en l'absence d'une autorisation judiciaire, la surveillance magnétoscopique constituait une violation de l'article 8 de la *Charte*, qui garantit le droit à la protection contre les fouilles, les perquisitions ou les saisies abusives. L'arrêt est particulièrement remarquable en ce qu'il élargit la définition du droit à la vie privée en y englobant celui de ne pas faire l'objet d'une surveillance magnétoscopique systématique par des agents de l'État. La Cour suprême a conclu que le droit à la vie privée doit être protégé par des instances judiciaires indépendantes, et qu'on ne peut laisser la police décider quand avoir recours à la surveillance magnétoscopique.

Dans les motifs de jugement de la majorité, le juge La Forest a précisé clairement que toutes les formes de surveillance électronique auxquelles des agents de l'État ont recours sans autorisation judiciaire constituent des violations de l'article 8 de la *Charte*:

> ... le droit général à la protection contre les fouilles, les perquisitions ou les saisies abusives garanti par l'art. 8 doit évoluer au rythme du progrès technologique et, par conséquent, nous assurer une protection constante contre les atteintes non autorisées à la vie privée par les agents de l'État, peu importe la forme technique que peuvent revêtir les divers moyens employés. (p. 6)

Par suite de l'arrêt *Wong*, les tribunaux ne peuvent plus se fonder sur le critère de l'analyse fondée sur le «risque couru» par la personne qui fait l'objet de la surveillance non autorisée. Comme le juge La Forest l'a déclaré:

> ... la vie privée serait mal protégée si le caractère raisonnable de notre attente en matière de respect de la vie privée dépendait de la question de savoir si nous nous sommes exposés à la surveillance électronique. Compte tenu de l'état avancé de la technologie en matière de surveillance, ce serait adopter une norme dépourvue de signification puisque, en dernière analyse, les ressources technologiques dont disposent les agents de l'État sont telles que nous courons maintenant le risque de voir nos propos enregistrés pratiquement chaque fois que nous parlons à une autre personne. (p. 7-8)

Par conséquent, même si l'accusé avait distribué de nombreuses invitations à se rendre à sa chambre d'hôtel et qu'il y avait donné accès à des inconnus, il n'avait pas perdu son droit au respect raisonnable de sa vie privée. La Cour suprême a clairement précisé que, même si l'on pourrait avoir recours sans mandat à la surveillance magnétoscopique des personnes qui se livrent à des activités illégales dans leurs chambres d'hôtel, la société s'opposerait à ce qu'on impose ce risque à tous ceux qui louent une chambre. Pour éviter ce risque, la Cour a jugé qu'elle devait interdire cette forme de surveillance.

À l'heure actuelle, contrairement à la surveillance électronique, il n'existe aucune procédure par laquelle la police doit obtenir une autorisation pour faire de la surveillance magnétoscopique. La Cour suprême était très consciente de l'entrave que sa décision allait imposer aux policiers, mais elle n'en a pas moins jugé que seul le Parlement devrait décider dans quelles circonstances ils peuvent porter atteinte à la vie privée en ayant recours à la surveillance magnétoscopique.

Le juge La Forest l'a bien dit:

> Selon moi, les tribunaux négligeraient leur rôle de protecteurs de nos libertés fondamentales s'ils devaient usurper le rôle du législateur et prétendre sanctionner la surveillance magnétoscopique en adoptant à cette fin un code de procédure conçu pour une technologie de surveillance complètement différente. C'est au législateur et à lui seul qu'il revient d'établir les conditions dans lesquelles les organismes d'application de la loi peuvent avoir recours à la technologie de surveillance magnétoscopique pour combattre la criminalité. Il en est de même pour toute nouvelle technologie que le progrès de la science mettra à la disposition de l'État dans les années à venir. (p. 23)

Il est certain que le gouvernement légiférera pour que la police puisse obtenir l'autorisation judiciaire d'avoir recours à la surveillance magnétoscopique. Ce serait la façon logique de procéder, étant donné que personne ne conteste que, pour appliquer la loi, il faut pouvoir avoir recours à ce moyen de surveillance. Toutefois, comme il le fait pour la surveillance électronique, le Commissaire à la protection de la vie privée invite instamment le Parlement à faire en sorte que toute procédure qu'il adoptera face à l'obtention d'une autorisation judiciaire pour fins de surveillance magnétoscopique, protège la vie privée des innocents.

Les téléphones cellulaires et la protection de la vie privée

Les Canadiens ont appris - parfois douloureusement - que les conversations faites par téléphone cellulaire peuvent être interceptées.

En Colombie-Britannique, un ministre provincial a démissionné après (qu'un journal?) eut imprimé des extraits de conversations téléphoniques qu'il avait eues dans sa voiture. Certaines des délégations provinciales à la conférence constitutionnelle du lac Meech soupçonnaient que leurs communications par téléphone cellulaire avaient été interceptées. Une Société provinciale d'énergie s'est retrouvée dans l'embarras quand quelqu'un a intercepté et publié les propos qu'un de ses employés avait tenus sur des leaders de la communauté à son téléphone cellulaire.

Face à cette nouvelle menace pour la vie privée, le Commissaire s'est posé deux questions:

- La *Loi sur la protection des renseignements personnels* protège-t-elle les conversations téléphoniques cellulaires?

- Les institutions fédérales, et notamment les organismes fédéraux d'application de la loi, restent-ils toujours dans la légalité lorsqu'ils interceptent des conversations de ce genre?

La Cour suprême a clairement déclaré que, lorsqu'ils n'ont pas obtenu l'autorisation judiciaire voulue, les agents de l'État ne peuvent pas soumettre les citoyens à une forme quelconque d'écoute électronique. S'ils le faisaient, ils se rendraient coupables de «perquisitions ou de saisies abusives». En effet, ils nous priveraient de notre droit à une protection raisonnable de notre vie privée, ce qui constituerait une violation de l'article 8 de la *Charte canadienne des droits et libertés*.

L'État ne peut plus présumer qu'un citoyen a renoncé à son droit à la protection de sa vie privée simplement parce qu'il «court le risque» d'être mis sous surveillance, par exemple en utilisant un mode de communication qu'il sait susceptible d'être intercepté. La Cour suprême a jugé que cette présomption fait courir un plus grand risque à notre société, en ce sens que si les agents de l'État pouvaient faire de la surveillance électronique sans mandat approprié, ils porteraient un si dur coup à la protection de notre vie privée que notre société ne pourrait plus être libre et ouverte.

Cette conclusion du plus haut tribunal du pays a des implications directes pour la *Loi sur la protection des renseignements personnels*, qui impose de nombreuses restrictions à la collecte des renseignements personnels par une institution fédérale, la principale (article 4) étant que seuls les renseignements «...qui ont un lien direct avec ses programmes ou ses activités» peuvent être recueillis par l'institution.

Cette disposition peut recevoir différentes interprétations dans des cas précis, mais elle ne peut absolument pas être interprétée de façon à justifier la collecte de renseignements personnels d'une façon qui, autrement, serait illégale. En outre, toute collecte de renseignements personnels contrairement à la *Charte* enfreint aussi la *Loi sur la protection des renseignements personnels*.

La *Loi sur la protection des renseignements personnels* entre en jeu lorsque des organismes d'enquête fédéraux interceptent des conversations faites par téléphone cellulaire. C'est pour cette raison que le Commissaire tient à s'assurer que toutes les interceptions effectuées par des organismes fédéraux le sont conformément à la Loi.

Le Commissaire fait enquête sur cette question, et il compte publier les résultats de ses travaux dans son prochain rapport annuel.

Ce qu'il y a de plus inquiétant encore, selon le Commissaire, c'est l'absence de contrôle légal portant sur les interceptions par les citoyens des conversations transmises par téléphone cellulaire. Un commentateur a décrit la situation en ces termes:

> L'utilisateur moyen d'un téléphone cellulaire est peut-être prêt à accepter d'entendre une autre conversation sur sa ligne, mais il serait probablement secoué d'apprendre que l'on peut délibérément écouter des conversations avec un équipement aussi simple qu'un vieux téléviseur capable de capter la fréquence UHF des téléphones cellulaires. (*Network Newsletter*, Vol. 10, n^{o} 24, 30 juillet 1990, p. 1)

La Cour suprême a réuni un ensemble de dispositions juridiques protégeant les citoyens contre l'écoute de leurs conversations téléphoniques cellulaires par des agents de l'État, mais la *Charte* ne contient rien qui puisse contrôler le comportement d'un particulier. En outre, il est loin d'être sûr que les dispositions du *Code criminel* qui interdisent l'interception secrète des communications privées s'appliquent aux communications téléphoniques cellulaires. Après tout, ces communications sont transmises par radio et, par conséquent, il se peut qu'elles ne puissent être considérées comme «privées».

Dans certaines instances, notamment en Californie, les législateurs ont adopté des lois interdisant à la fois l'interception des communications cellulaires et la vente ou l'achat d'un dispositif d'écoute capable de les capter. Le Congrès des États-Unis est même saisi d'un projet de loi d'une portée plus vaste encore sur les communications informatiques et radio (H.R.3378 et S.1667). En vertu de ce projet de loi, il serait illégal d'intercepter une conversation transmise par un téléphone d'auto, à l'instar de toute autre communication radio privée.

Bien sûr, la loi ne peut pas nous assurer que nos conversations par téléphone cellulaire demeureront privées. En fait, certains prétendent que l'adoption d'une loi qui nous offrirait cette protection pourrait inspirer aux utilisateurs de ces téléphones un faux sentiment de sécurité, ce qui serait tout à fait contraire à l'intention du législateur. Le Commissaire n'est pas d'accord; selon lui, il est absolument vital que le Parlement agisse rapidement pour protéger la vie privée des utilisateurs de téléphones cellulaires. L'élimination des fils téléphoniques ne doit pas entraîner celle de la protection de notre vie privée.

La protection de la vie privée dans le secteur privé

Dans notre société où règne l'ordinateur, la distribution de l'information est illimitée. Et pourtant, le Canada se contente d'une législation qui assure une certaine protection contre les utilisations abusives de l'information dans l'administration fédérale et dans une partie des administrations provinciales, sans aucun mécanisme équivalent dans le secteur privé.

En Europe, la situation est très différente. La plupart des pays membres de la Communauté économique européenne (CÉE) se sont donné des mécanismes de protection des renseignements personnels tant dans le secteur privé que dans le secteur public. En outre, les autorités s'affairent actuellement pour renforcer et harmoniser ces mécanismes en vue de l'unification de l'Europe, en 1992.

Pourquoi comparer le Canada à l'Europe? Eh bien, parce que ces différences ont d'importantes conséquences pour les entreprises canadiennes qui font des affaires en Europe ... ou qui espèrent en faire. En effet, si le Canada n'adopte pas de législation comparable à la leur pour assurer la protection des données dans le secteur privé, les pays européens risquent de ne plus autoriser le transfert au Canada d'information concernant leurs ressortissants. La législation européenne sur la protection des données pourrait devenir une barrière non tarifaire qui réduirait nettement les possibilités des entreprises canadiennes de traiter avec ce qui promet de devenir l'un des plus grands blocs commerciaux du monde.

Le danger est très réel: il suffit pour en être convaincu d'étudier le projet de directive de la CÉE sur la protection des données personnelles des individus, présenté en juillet 1990. Si ce projet est adopté, tous les pays membres de la CÉE devront l'appliquer à partir du 1er janvier 1993. La directive a deux objectifs globaux:

- établir un mécanisme assurant une protection uniforme et de qualité de la vie privée tant dans les secteurs public que privé;

- éliminer tous les obstacles au libre échange de données personnelles entre les pays membres.

Le hic, c'est que la directive a des implications alarmantes pour les pays qui ne sont pas membres de la CÉE et qui n'assurent pas une protection de la vie privée satisfaisant aux normes européennes. En effet, l'article 24 du projet de directive interdit aux membres de transférer des données personnelles à toute compétence qui n'en assure pas une protection satisfaisante. Compte tenu de la loi en ce moment, il est fort peu probable que le secteur privé au Canada puisse démontrer un niveau acceptable de protection de renseignements.

Toutes les instances européennes intéressées - l'Organisation de coopération et de développement économiques (OCDE), le Conseil de l'Europe, la CÉE et les organismes européens de protection des données - sont parfaitement conscientes des implications du projet de directive pour les pays qui ne sont pas membres de la CÉE. Elles savent que le Canada - et les États-Unis, à ce compte-là - reconnaissent les principes applicables à la protection des données (le Canada a signé les lignes directrices de l'OCDE sur la protection des renseignements personnels). Elles savent aussi que les autorités gouvernementales nord-américaines préfèrent laisser le secteur privé s'autoréglementer.

Toutefois, les Européens n'ignorent pas que l'autoréglementation n'a pas connu de succès retentissants, et que seule une poignée d'entreprises canadiennes et américaines ont adopté des codes valables de protection des données.

Bref, même si les Européens reconnaissent qu'il peut y avoir plus d'une façon d'assurer la protection des données, par exemple grâce à des codes d'autoréglementation entre eux, ils ne sont pas disposés à accepter de compromis sur le plan des principes. Par conséquent, les organismes européens de protection des données n'autoriseront plus le transfert des renseignements personnels à des pays qui n'adhèrent que du bout des lèvres au principe de la protection de ces renseignements.

C'est un avertissement en bonne et due forme que le Commissaire à la protection de la vie privée du Canada s'est fait servir par les responsables européens de la protection des renseignements personnels.

L'an dernier, le Commissaire a recommandé dans son rapport annuel que le Parlement modifie la *Loi sur la protection des renseignements personnels* pour obliger les entreprises privées de compétence fédérale à élaborer, à enregistrer et à mettre en vigueur des codes de protection de la vie privée fondés sur les principes internationalement reconnus qui ont été établis par les lignes directrices de l'OCDE.

Ses discussions avec les autorités européennes chargées de la protection des données ont convaincu le Commissaire que des codes d'autoréglementation seraient acceptables, à condition de reposer sur une base juridique comme celle-là.

Il s'ensuit que, pour le Commissaire, la mise en oeuvre de cette recommandation est urgente, car non seulement les Canadiens méritent-ils de bénéficier de toute cette protection de leur vie privée, mais encore les entreprises canadiennes risquent-elles d'être sérieusement désavantagées lorsqu'elles voudront continuer après 1992 à traiter avec des firmes de l'Europe.

Des débuts encourageants

Il ne faut pas passer les réussites du secteur privé sous silence du seul fait qu'elles sont rares. Ainsi, en décembre 1990, l'Association des banquiers canadiens (ABC) a approuvé un code de protection des renseignements personnels digne d'être cité en exemple, dans lequel elle a précisé les normes minimales de protection des renseignements personnels des clients, que ses membres sont tenus d'appliquer.

Le code de l'ABC garantit aux clients le droit d'accès aux renseignements personnels qui les concernent et le droit aussi de les faire corriger. En outre, il contrôle les modalités de collecte, de conservation, d'utilisation, de divulgation, d'élimination et de sécurité applicables aux dossiers des clients.

Les banques ont toujours su admirablement protéger la confidentialité de l'information relative à leurs clients, mais il reste que le code assurera désormais aux clients un meilleur contrôle des renseignements financiers qui les concernent.

Cela dit, les promoteurs de la protection de la vie privée, dont le Commissaire, ont constaté quelques lacunes; par exemple, le code de l'ABC ne donne pas aux clients l'accès aux opinions ou aux jugements à leur endroit qui figurent dans leur dossier, mais seulement aux renseignements factuels sur eux-mêmes. Le Commissaire espère que le code sera modifié afin de combler les carences. Malgré ces réserves, le Commissaire perçoit d'une manière positive les efforts fournis par l'ABC.

Bell Canada mérite des éloges, elle aussi, car elle s'est donné un code de protection des renseignements personnels qui reconnaît des droits et assure une protection à ses employés tout autant qu'à ses clients, et qu'elle ne limite pas leur accès aux seules données factuelles.

Dans un monde où les télécommunications font l'objet d'une concurrence de plus en plus féroce, ce souci manifeste de protéger la vie privée des clients et des employés aura sûrement un effet d'entraînement. Le Commissaire presse les autres entreprises du secteur des télécommunications d'emboîter le pas à Bell. Il suivra la situation et signalera les progrès réalisés.

Enfin, l'Association canadienne du marketing direct (ACMD) a récemment annoncé l'adoption de nouvelles mesures de protection de la vie privée, en lançant son «Opération intégrité», le 13 février 1991. L'ACMD a renforcé les dispositions de protection de la vie privée de son code d'éthique, en s'engageant à donner aux consommateurs de meilleurs moyens d'échapper aux intrusions dans leur vie privée des entreprises d'envois postaux directs et de télémarketing.

L'Opération intégrité donne aux consommateurs la possibilité de demander que leur nom soit rayé des listes d'envois postaux et des répertoires téléphoniques des membres de l'ACMD. En outre, elle interdit à ceux-ci d'inclure dans les listes qu'ils louent des renseignements de nature délicate (médicaux, financiers ou judiciaires, ou encore sur des questions d'assurances). L'ACMD a aussi mis sur pied un groupe de travail formé de représentants en vue de son secteur d'activité, qui étudieront les implications du marketing direct en matière de protection de la vie privée, afin d'élaborer d'autres politiques sur le transfert de données.

L'ACMD a communiqué ses activités dans ce domaine au Commissaire, qui se fera un plaisir de poursuivre le dialogue avec elle.

Tests biomédicaux

Le dépistage antidrogue

Les lecteurs assidus du rapport annuel se rappelleront que, l'an dernier, le Commissaire avait fortement déconseillé à l'administration fédérale de généraliser le dépistage antidrogue pour contrer le fléau des substances interdites.

Dans son étude en profondeur, intitulée *Le dépistage antidrogue et la vie privée*, le Commissaire a examiné différents milieux, notamment ceux des transports, des établissements correctionnels, des forces armées et des sports. Il a constaté qu'un grand nombre de projets de dépistage envisagés par l'administration fédérale risquaient de violer la *Loi sur la protection des renseignements personnels* et la *Charte canadienne des droits et libertés*, voire des principes plus fondamentaux encore de protection de l'intégrité individuelle.

Il est clair que la situation a évolué depuis, et qu'on envisage des mesures de protection de la vie privée, qui était menacée par le dépistage antidrogue. Le Commissariat a été consulté par Santé et Bien-être social Canada au sujet d'éventuels protocoles de dépistage. Il a répondu au rapport de l'administration fédérale sur le dépistage antidrogue dans le secteur des transports, et il a discuté avec le Service correctionnel du Canada (SCC) le règlement que celui-ci a proposé en vue du dépistage antidrogue dans les pénitenciers fédéraux.

Transports Canada n'envisage plus de soumettre au hasard tous les titulaires de postes reliés à la sécurité des transports à un test de dépistage des drogues obligatoire. Le dernier projet de règlement du SCC est de loin préférable aux versions antérieures, qui avaient été rejetées en 1989 par la division de première instance de la Cour fédérale, dans *Jackson*. Enfin, les protocoles de dépistage de Santé et Bien-être social Canada prévoient désormais des méthodes de prélèvement d'échantillons d'urine qui portent moins atteinte à la vie privée qu'auparavant.

Malheureusement, certains aspects de la politique de dépistage antidrogue dans le secteur des transports restent inquiétants. Transports Canada tient toujours à imposer des tests d'analyse d'urine préalablement à l'emploi pour les employés nouvellement recrutés ou mutés, ainsi qu'à l'occasion des examens médicaux périodiques, et cela même si ses propres recherches n'ont révélé aucune consommation sérieuse de substances pouvant représenter une menace pour la sécurité dans ce secteur. Il faut ajouter que l'analyse d'urine ne fournit que des renseignements très limités, à savoir qu'une personne a consommé telle ou telle substance dans un passé récent, sans préciser avec quelle fréquence et sans non plus confirmer que les facultés du sujet étaient altérées au moment du test, ou, chose plus importante encore, si elles le sont encore maintenant.

L'obligation de subir des tests de dépistage des drogues dans ces conditions est contraire à la *Loi sur la protection des renseignements personnels* et elle risque d'être interdite pour peu qu'elle soit contestée en vertu de la *Charte canadienne des droits et libertés*. Bref, ces tests ne devraient être administrés que si l'on a des motifs raisonnables de croire que quelqu'un consomme de la drogue - ou encore après un accident.

Il est regrettable de constater que le ministère de la Défense nationale (MDN) soit toujours bien déterminé à appliquer son projet d'astreindre les militaires à des tests de dépistage des drogues et ce, en dépit des recommandations du Commissaire et des conclusions du comité des transports sur le dépistage obligatoire effectué au hasard. Cela dit, le MDN compte faire subir des tests lorsqu'il aura des motifs valables de le faire, dans le cadre d'enquêtes menées à l'occasion d'un accident ou d'un incident, pendant une période de surveillance à la suite d'un test de dépistage des drogues s'étant révélé positif, et enfin pour recueillir des données. Il prévoit de plus administrer des tests obligatoires au hasard dans le cas des militaires affectés à des unités opérationnelles ou occupant des postes reliés à la sécurité.

Et ce n'est pas tout. Condition physique et Sport amateur a réagi au rapport Dubin sur la consommation de drogues chez les athlètes amateurs en mettant sur pied une nouvelle organisation antidopage financée essentiellement par l'administration fédérale, quoique n'en faisant pas partie. Cette organisation doit coordonner tous les plans antidopage dans le domaine du sport et administrer un programme d'envergure accrue pour soumettre les athlètes à des tests de dépistage des substances proscrites.

L'un des éléments fondamentaux du plan envisagé consiste à soumettre les athlètes à des tests de dépistage «à l'improviste», indépendamment des compétitions. En fait, on prévoit jusqu'à 3000 tests (par année, sans doute), dont la majorité seraient faits «à l'improviste.».

Comme l'organisation antidopage ne sera pas un organisme fédéral, la *Loi sur la protection des renseignements personnels* ne s'y appliquera pas. Il se peut qu'on ait délibérément opté pour cette solution afin de contourner la Loi, mais l'approche de l'organisation, telle que le Ministre responsable l'a annoncée, soulève fatalement des objections fondées sur le respect de la vie privée. Les athlètes risquent de se retrouver à peu près complètement privés de droits à cet égard, à telle enseigne que le Commissaire a l'intention d'en discuter avec les responsables de Condition physique et Sport amateur.

En fait, la plupart des programmes de dépistage antidrogue continuent de préoccuper le Commissaire, qui estime que les programmes gouvernementaux sont un mauvais exemple pour le secteur privé, et que, dans la plupart des cas, ils ne semblent pas conformes à la *Loi sur la protection des renseignements personnels*. Il reste que le Commissariat n'a pas de meilleurs recours que de critiquer publiquement ces programmes, car il ne peut contraindre l'administration fédérale à respecter la Loi.

Le dépistage du VIH

Le personnel du Commissariat continue à répondre aux demandes d'information et à faire enquête sur les plaintes concernant le respect de la vie privée dans le contexte du VIH et du SIDA. Étant donné que les demandes portent souvent sur des questions ou sur des organismes qui ne relèvent pas de la *Loi sur la protection des renseignements personnels*, le personnel tente d'aiguiller les appels vers les autorités responsables.

La pierre angulaire du travail du Commissariat en matière de VIH et de SIDA est un rapport publié en 1989 et intitulé *Le SIDA et la Loi sur la protection des renseignements personnels*. Le personnel a en outre contribué à l'élaboration des «Guidelines on Ethical and Legal Considerations in Anonymous Unlinked HIV Seroprevalence Research», en 1988. Ces lignes directrices ont été publiées dans le *Canadian Medical Journal*, en 1990. En février 1991, le Commissariat a participé à la révision des lignes directrices originales.

En novembre 1990, le Commissariat a été représenté à la réunion du Conseil des organisations internationales des sciences médicales, où il a été question d'un code d'éthique de la recherche épidémiologique, y compris la recherche sur le VIH et le SIDA.

Le travail du Commissariat sur le VIH et le SIDA est complété par des recherches effectuées en Ontario. La Commission de réforme du droit de l'Ontario procède en effet à une vaste étude sur les implications juridiques et, dans une certaine mesure, sur l'éthique du dépistage du VIH et du SIDA. Le Commissaire à l'information et à la protection de la vie privée de l'Ontario a quant à lui publié deux rapports à ce sujet, l'un sur le VIH et le SIDA et la protection de la vie privée, et l'autre sur le VIH et le SIDA et le milieu de travail.

Le dépistage génétique

La génétique moderne nous offre de grandes possibilités d'identification des troubles génétiques, dont quelques-uns susceptibles d'être traitables. Toutefois, le dépistage génétique soulève de graves questions de protection de la vie privée, en ce qu'il risque de révéler des renseignements très délicats sur la personne qui subit les tests et sur ceux et celles qui partagent son bagage génétique. Les tests de dépistage de ce genre font appel à trois techniques.

1) Filtrage génétique: Examen d'un échantillon de tissu ou de sang d'un individu pour y dépister les gènes ou «marqueurs» génétiques indiquant la présence ou le risque d'un trouble génétique ou d'une autre caractéristique physique.

2) Contrôle génétique: Recherche de changements génétiques ou chromosomiques pouvant résulter de l'exposition dans le milieu du travail ou dans le milieu ambiant à des substances chimiques ou à divers phénomènes (radiation ou émanations de matières plastiques, par exemple).

3) Analyse pathologique de l'ADN: Appelée communément, identification par l'ADN. Cette technique consiste en une comparaison génétique d'échantillons. C'est ainsi qu'on peut prouver que la composition génétique du sang trouvé sur le lieu d'un crime correspond à celle du sang d'un suspect. Ce genre d'analyse peut aussi prouver l'affiliation génétique dans les affaires d'immigration ou de paternité.

Les autres formes d'analyse biotechnologique, comme le dépistage des anticorps du VIH et du SIDA ou des drogues ne révèlent qu'un seul fait, l'infection au VIH ou la consommation de drogues dans le passé. Le dépistage génétique, par contre, peut révéler des centaines de données sur un individu ou sur ses parents, de la certitude d'être atteint d'une maladie ou d'une affection invalidante ou mortelle, comme la chorée de Huntington ou la fibrose kystique, jusqu'au risque de développer des troubles psychiatriques, comme d'être maniaco-dépressif, ou d'être prédisposé à avoir des taux élevés de cholestérol, à faire de l'hypertension ou à être atteint de certains types de cancer.

Le dépistage génétique est sur le point de devenir une question centrale dans les domaines de la reproduction humaine (dépistage avant la conception et dépistage prénatal et néo-natal), de l'emploi (filtrage et contrôle), de l'accès aux services gouvernementaux et privés (éducation, assurances, crédit), des enquêtes criminelles, des soins médicaux de routine et de la recherche.

Les énormes possibilités actuelles et potentielles d'utilisation de l'information obtenue grâce au dépistage génétique ont amené le Commissaire à étudier ses implications pour la protection de la vie privée. Il devrait avoir terminé son étude à la fin du printemps de 1991. Toutefois, il semble qu'une conclusion s'impose déjà. Le dépistage génétique a de telles implications pour la protection de la vie privée que le gouvernement doit se demander s'il devrait directement réglementer son utilisation dans le secteur privé.

La réforme électorale: une liste électorale permanente

Il peut être question de vie privée quand on s'y attend le moins, comme lorsque le gouvernement a chargé une Commission royale d'enquête d'étudier l'opportunité d'une refonte de la législation électorale canadienne.

La Commission d'enquête devait étudier la procédure électorale et les modalités de financement des partis et des campagnes, ainsi que la possibilité d'une liste électorale permanente grâce à laquelle nous n'aurions plus besoin chaque fois d'une énumération de porte à porte.

L'élimination de l'énumération de porte à porte aurait des avantages. Toutefois, la solution envisagée touchant cette pratique qui prend du temps et qui gonfle le coût déjà élevé des élections fédérales au Canada ne doit pas être adoptée à la légère.

La Commission a entendu des propositions axées sur des combinaisons de renseignements provenant de divers fichiers d'information fédéraux, comme les dossiers de l'impôt sur le revenu, les registres de la citoyenneté, les avis de changement d'adresse de la Société canadienne des postes, les formulaires de recensement et les registres des pensions. On devait aussi présenter d'autres propositions fondées sur l'intégration des registres provinciaux de la santé et des dossiers des conducteurs. Enfin, l'idée d'obliger les électeurs à avoir une carte d'identité spéciale ou à produire leur numéro d'assurance sociale (NAS) a séduit beaucoup de monde.

Tout cela a incité le Commissaire à la protection de la vie privée à écrire à la Commission d'enquête pour lui demander de réfléchir aux répercussions éventuelles de ses recommandations sur la vie privée.

Le Commissaire s'inquiète des applications des nouvelles collections (ou couplages) de renseignements personnels sur une grande échelle. Une liste électorale permanente comme celle qu'on envisage deviendrait une sorte de registre de la population qui serait vraiment dangereux pour les droits et libertés de la personne. L'expérience acquise en temps de guerre prouve que, même au Canada, on fera mauvais usage de ces listes, pour traiter injustement des groupes importants de citoyens et pour les arrêter, les emprisonner et confisquer leurs biens.

En outre, s'il fallait que cette liste existe, il y aurait des pressions croissantes pour qu'elle soit mise à la disposition de tous les organismes gouvernementaux imaginables, à des fins qui n'auraient rien à voir avec les élections. Il faudrait absolument que son utilisation soit limitée à cette seule fin, et que les données qu'elle contiendrait soient strictement confidentielles.

Le mécontentement croissant que suscitent les utilisations injustifiées du NAS reflète la résistance des citoyens aux projets d'identification et d'enregistrement à l'échelle nationale, et cette résistance se renforcerait si l'on devait se servir du NAS pour faire le pont entre différentes bases de données et pour confirmer le droit de vote de chaque citoyen.

Enfin, la *Loi sur la protection des renseignements personnels* interdit l'accès aux autres bases de données fédérales en vue de la création d'une liste de ce genre, dont l'établissement nécessiterait la promulgation d'une loi fédérale qui la soustrairait à l'application de la *Loi sur la protection des renseignements personnels*. Le Commissaire n'appuirait jamais une démarche pareille.

Les citoyens du monde entier en ont assez d'être comptés, enregistrés et contrôlés par l'État. La création d'une liste permanente des électeurs risque de susciter un profond malaise. Il serait ironique que le processus électoral, qui est le fondement même de la démocratie, devienne un mécanisme qui fera pencher la balance plus encore du côté de l'État, aux dépens du citoyen.

Le Commissaire ne veut pas s'opposer au progrès, mais il tient à poser des questions pertinentes avant que ce projet n'aille trop loin. Ses observations ont été bien accueillies par la Commission d'enquête, qui se propose de rendre son rapport public à l'automne de 1991.

La protection de la vie privée et l'intérêt public: un équilibre difficile à protéger

Globalement, la *Loi sur la protection des renseignements personnels* interdit aux institutions fédérales de communiquer les renseignements personnels qui sont sous leur contrôle à défaut du consentement de la personne concernée. Toutefois, la Loi admet aussi treize exceptions à la règle.

L'une des treize est de portée très générale, ce qui la rend difficile à appliquer et ouvre la porte à de nombreux abus. C'est le sous-alinéa 8(2)m)(i), qui autorise la divulgation des renseignements personnels à toutes les fins autres que celles auxquelles ils ont été recueillis, dans les cas où, de l'avis du responsable de l'institution:

> des raisons d'intérêt public justifieraient nettement une éventuelle violation de la vie privée...

Au cours de la dernière année, l'institution qui a le plus fréquemment invoqué cette disposition a été le Service correctionnel du Canada (SCC). Le problème se pose quand des incidents survenus dans le contexte carcéral, comme des évasions, des morts violentes ou des prises d'otages, mènent à des enquêtes internes qui aboutissent à des rapports contenant des renseignements personnels à la fois sur les détenus et sur les fonctionnaires impliqués du SCC.

Par conséquent, le SCC doit tenir compte des interdictions imposées par la *Loi sur la protection des renseignements personnels* avant de communiquer ces rapports. Il se peut fort bien qu'il veuille les distribuer afin de conserver la confiance que le public accorde au système correctionnel, et il peut aussi avoir besoin d'en fournir des exemplaires aux journalistes qui les ont réclamés en vertu de la *Loi sur l'accès à l'information*, ainsi qu'à des députés et sénateurs ou à des comités parlementaires désireux de les étudier afin d'évaluer la qualité globale de l'administration correctionnelle. Dans ces cas-là, le SCC retire des rapports tous les renseignements considérés comme inconsultables en vertu de la *Loi sur l'accès à l'information*, de même que les détails personnels délicats ou non pertinents.

Bref, le SCC s'efforce de divulguer seulement les renseignements personnels nécessaires pour satisfaire au critère d'intérêt public établi par la *Loi sur la protection des renseignements personnels* et pour donner au public une image claire de ce qui s'est passé.

Une fois que les renseignements ont été filtrés à la satisfaction du Commissaire du Service correctionnel et du Solliciteur général, ceux-ci avisent le Commissaire à la protection de la vie privée de leur intention de les communiquer (à l'avance, si c'est possible sans leur causer trop de difficultés). Quand le Commissaire reçoit le préavis, il décide s'il s'agit d'une communication pour des raisons d'intérêt public qui «justifieraient nettement une éventuelle violation de la vie privée». S'il n'est pas de cet avis, il en informe le SCC. Il convient toutefois de souligner que le Commissaire n'a pas le pouvoir d'empêcher la communication des renseignements, mais seulement de prévenir les personnes intéressées qu'ils seront divulgués.

Il est extrêmement difficile d'appliquer le critère des raisons d'intérêt public, comme on l'a vu dans deux cas de communications dont le Commissaire a fait état dans son rapport de l'an dernier («Communication des rapports portant sur l'évasion de deux détenus»). Le Comité permanent de la Justice et du Solliciteur général a tenu à se renseigner sur les événements ayant entouré ces deux incidents qui avaient fait la manchette, à savoir l'évasion du pénitencier de Dorchester, au Nouveau-Brunswick, d'un dénommé Allan Légère (qui aurait assassiné une personne après son évasion) et celle de Daniel Gingras, qui avait profité d'une permission de sortie d'une journée pour s'enfuir. Par la suite, il avait assassiné deux personnes.

Le SCC avait déjà communiqué aux médias des versions épurées des rapports d'enquête, et c'est cette version des rapports qu'il a remise au Comité. Toutefois, celui-ci a réclamé les versions intégrales, et il a ordonné au Solliciteur général de les lui faire remettre.

Le Solliciteur général a refusé d'obéir, en alléguant que la *Loi sur la protection des renseignements personnels* lui interdisait de communiquer les renseignements demandés. Son refus a fait l'objet d'une question de privilège à la Chambre des communes, et la question a fini par être renvoyée au Comité permanent des privilèges et des élections. Dans son témoignage devant le premier Comité, le Solliciteur général a déclaré qu'il était tenu de respecter le sous-alinéa 8(2)m)(i) de la *Loi sur la protection des renseignements personnels*, de sorte que, avant de communiquer les renseignements demandés, il devait être convaincu qu'il était essentiel de le faire pour des raisons d'intérêt public qui justifieraient clairement une éventuelle violation de la vie privée. Il a ajouté qu'il n'était pas sûr que la *Loi sur la protection des renseignements personnels* l'autorisait à accéder à la demande du Comité, qui voulait étudier à huis clos la version intégrale des rapports.

Le Commissaire par intérim à la protection de la vie privée a comparu devant le Comité des privilèges. Il a applaudi à la détermination du Solliciteur général de protéger la vie privée des personnes mentionnées dans les rapports, mais il a conclu que le Ministre interprétait la Loi de façon trop restrictive. En effet, le sous-alinéa 8(2)m)(i) lui donne de toute évidence le pouvoir de décider si la communication de la version intégrale des rapports au Comité de la Justice siégeant à huis clos sert l'intérêt public. Le Commissaire par intérim a ajouté qu'il n'était pas du tout contraire à l'esprit de cette disposition de la Loi que le Ministre juge d'intérêt la communication des renseignements au Comité, à condition qu'elle ait lieu dans des conditions garantissant la confidentialité des parties «sensurées».

Cette histoire n'est pas finie, car le Comité des privilèges n'a pas terminé ses délibérations, et le Commissaire à la protection de la vie privée n'a pas non plus mené à bien son enquête sur une plainte connexe.

«La vérité, toute la vérité et rien que la vérité»

N'oublions pas l'autre côté de la médaille: il est pour le moins inhabituel que le Commissaire à la protection de la vie privée rappelle publiquement aux institutions fédérales que le droit à la vie privée n'est pas absolu. Le fait est que la Loi reconnaît que la vie privée peut être violée si certains intérêts collectifs importants sont en jeu.

Être doctrinaire au point d'insister sur le caractère confidentiel de tous les cas risque de donner à la Loi une mauvaise réputation qu'elle ne mérite pas. Ces incidents mettant en cause le SCC en sont un bon exemple.

Bien que les raisons d'intérêt public invoquées par le SCC pour communiquer les deux rapports en question consistent à préserver la confiance que la population accorde au système correctionnel, il en a retiré des parties qui contiennent des critiques à l'endroit de certains membres de son personnel. Même si les mesures qu'il a prises pour protéger ces gens sont compréhensibles, le rapport «censuré» qui en résulte ne donne pas au public un compte rendu complet de l'incident.

S'il ne communique pas ce qui le fait mal paraître aussi bien que ce qui l'avantage, le SCC agit-il vraiment pour des raisons d'intérêt public? C'est précisément cette question qui continue à faire l'objet de discussions entre ses dirigeants et le Commissaire à la protection de la vie privée. Il nous semble que le SCC devrait n'invoquer la clause «d'intérêt public» que dans des cas extraordinaires, et s'en servir alors pour communiquer une information complète.

Direction des plaintes

Le nombre de plaintes a augmenté d'environ 10 p. 100 par année depuis que le Commissariat a fait ses débuts, il y a sept ans. La tendance s'est maintenue l'an dernier, car les 1239 plaintes reçues représentent une augmentation de 14 p. 100 par rapport aux 1086 de l'année précédente.

Plaintes portant sur la lenteur des réponses aux demandes

Dans ses rapports antérieurs, le Commissaire a parfois eu l'impression de faire un travail de Sisyphe, puisqu'il a dû constamment répéter ses critiques au sujet des longs délais de traitement des plaintes du Service correctionnel du Canada (SCC) et du ministère de la Défense nationale (MDN).

Les choses ont bien changé. Cette année, le nombre de plaintes de ce genre a nettement baissé, et c'est tout à l'honneur du SCC, qui a répondu aux critiques du Commissaire sur son rendement de l'an dernier par une refonte complète de ses méthodes de traitement des demandes.

Résultat? Une baisse étonnante de 200 p. 100 (de 214 à 50) du nombre de plaintes de ce genre portées contre le SCC. L'an dernier, ces plaintes à l'endroit du SCC représentaient 50 p. 100 de l'ensemble des plaintes portant sur les retards dont le Commissariat avait été saisi, et cette année, elles n'en représentent plus que 15 p. 100. Chapeau pour un travail bien fait!

La façon du MDN de traiter les rapports d'évaluation du rendement était elle aussi la cause de nombreuses plaintes de retards. Le problème était dû au fait que les militaires devaient présenter une demande officielle pour avoir accès à leurs évaluations, ce qui créait une charge de travail énorme et entraînait fatalement un arriéré. L'an dernier, le Commissaire a applaudi à la décision du MDN de traiter ces demandes sans formalités. Comme il l'avait prévu, le nombre de demandes adressées au MDN en vertu de la Loi a baissé de 20 p. 100, et la plus grande partie de cette baisse est directement attribuable à ce changement de politique, qui a fait chuter de 36 p. 100 (de 78 à 50) le nombre de plaintes de retards portées contre le MDN.

Les institutions gouvernementales s'efforcent de toute évidence de respecter les délais imposés par la Loi, et la tendance le démontre sans équivoque. Néanmoins, la raréfaction des ressources risque de tuer ces progrès dans l'oeuf. Le droit du citoyen d'avoir accès rapidement aux renseignements personnels qui le concernent ne devrait pas être sacrifié sur l'autel des restrictions budgétaires.

Code d'éthique sur les renseignements personnels

Bien que les plaintes portant sur des refus d'accès à l'information soient à la hausse, l'augmentation de 14 p. 100 constatée au cours de la dernière année est imputable à une importante poussée des plaintes concernant la collecte, l'utilisation et la divulgation des renseignements personnels, c'est-à-dire ce qu'on appelle un code d'éthique sur les renseignements personnels. Cette année, le nombre de plaintes de ce genre a grimpé en flèche, en établissant un record : 386, par rapport aux 173 de l'an dernier.

Une fois de plus, le problème semble être dû essentiellement aux conflits de travail à la Société canadienne des postes, qui donne l'impression d'appliquer sa nouvelle politique de gestion des congés avec beaucoup de fermeté. Les employés craignent qu'on ait recueilli indûment des renseignements médicaux qui les concernent et qu'on les ait utilisés pour gérer leur présence au travail.

Les dix grands

Le rapport de cette année contient une liste des dix plus gros «clients» du Commissariat, qui totalisent 80 p. 100 de sa charge de travail. Le Service correctionnel du Canada, qui dominait depuis le début pour le nombre de nouvelles plaintes, n'a été que trop heureux de céder cet «honneur» en 1990-1991 à la Société canadienne des postes.

		MOTIFS		
MINISTÈRE	TOTAL	ACCÈS	RETARD	AUTRE
Société canadienne des postes	239	40	54	145
Service correctionnel du Canada	165	77	50	38
Défense nationale	163	51	56	56
Emploi et Immigration Canada	128	61	44	23
Service canadien du renseignement de sécurité	77	67	9	1
Revenu Canada, Impôt	75	23	39	13
Transports Canada	67	43	17	7
Archives nationales du Canada	51	12	1	38
Gendarmerie royale du Canada	50	35	2	13
Santé et Bien-être social Canada	32	14	15	3
Autres	192	95	50	47
TOTAL	1,239	518	337	384

Le nombre des plaintes portées contre la Société canadienne des postes est passé de 97 l'an dernier à 237 cette année, tandis que les 165 plaintes portées cette année contre le SCC représentent moins de la moitié du «record» de 392 établi l'an dernier.

Une autre augmentation marquée s'est produite dans le cas d'Emploi et Immigration Canada, dont les 128 plaintes représentent le triple du total de l'an dernier pour cet organisme. Pour sa part, Transports Canada est revenu à un résultat plus près de la normale, avec 67 plaintes, alors qu'on n'en avait porté que 6 contre lui en 1989-1990. Il y a eu d'autres augmentations importantes du nombre de plaintes à l'endroit des Archives nationales, du MDN et du Service canadien du renseignement de sécurité (SCRS), sans qu'on sache très bien pourquoi. Par contre, le nombre de plaintes portées contre Santé et Bien-être social Canada et contre la GRC a baissé.

Prestation des institutions fédérales

Les plaintes peuvent être causées par plusieurs facteurs, comme une augmentation imprévue du nombre de demandes, tout simplement. En fait, une grande partie de ces facteurs sont totalement indépendants de la volonté des institutions responsables. La proportion des plaintes bien fondées est un indice plus significatif de la qualité de leur prestation.

Selon ce critère, la Gendarmerie royale du Canada distance de loin les autres institutions fédérales par la qualité de son rendement, car 5 seulement des plaintes portées contre elle se sont révélées bien fondées ou bien fondées et résolues, tandis que 16 n'étaient pas fondées et que 7 autres ont été abandonnées. C'est une baisse importante par rapport aux 19 plaintes bien fondées d'il y a 2 ans et aux 10 de l'an dernier, qui reflète le respect sincère de la GRC pour l'esprit et la lettre de la Loi. Son coordonnateur de l'accès à l'information et de la protection des renseignements personnels mérite d'ailleurs des éloges pour son engagement personnel de réduire le nombre de plaintes bien fondées.

Pour leur part, les Archives nationales continuent de maintenir leurs normes élevées, car 4 seulement des 23 plaintes portées contre elles se sont révélées bien fondées, et 3 des 4 ont été résolues.

Au risque de friser l'inconséquence, nous devons aussi féliciter la Société canadienne des postes, qui s'est pourtant classée au premier rang pour le nombre de plaintes, puisque 50 seulement des 230 plaintes portées contre elle étaient bien fondées, et que 37 des 50 ont été résolues.

Bien que le SCC semble avoir surmonté son problème de respect des délais, il conserve la pire proportion de plaintes bien fondées des grandes institutions fédérales, avec 64 p. 100 (103 sur 162). Sous cet aspect, Emploi et Immigration Canada et Revenu Canada (Impôt) se sont classés ex aequo au deuxième rang, avec 60 p. 100; le MDN les a suivis de près, avec 58 p. 100 de plaintes bien fondées.

Les enquêteurs du Commissariat ont mené 1008 enquêtes sur des plaintes (551 non fondées, 402 bien fondées et 55 abandonnées).

Cette année, les plaintes ont été groupées en trois grandes catégories, soit les plaintes concernant l'accès, c'est-à-dire les difficultés éprouvées par les citoyens désireux de consulter les dossiers qui les concernent; les plaintes portant sur la protection des renseignements personnels, c'est-à-dire le code d'équité en la matière (collecte, utilisation et divulgation conformes aux règles) et les plaintes concernant les retards, tant pour la première réponse à une demande que pour les prolongations de délai.

D'autres ressources, de grâce!

Même si les enquêteurs ont étudié plus de 1000 plaintes au cours de l'exercice, ce qui correspond à la norme des trois dernières années, il en restait 589 en souffrance à la fin de l'année, soit une augmentation de 38 p. 100 par rapport à l'an dernier. Bref, le Commissariat se retrouve avec un arriéré après avoir trimé si dur, il y a deux ans, pour éliminer celui d'alors. Le problème s'aggravera encore si l'augmentation de 10 p. 100 du nombre de plaintes prévue pour 1991-1992 se concrétise, ce qui sera probablement le cas, s'il faut en croire l'augmentation de 14 p. 100 de cette année.

	RÉSULTATS				
MOTIFS	Bien fondée	Bien fondée; résolue	Non fondée	Abandonnée	TOTAL
ACCÈS	30	70	320	16	436
Accès	27	69	305	16	417
Correction/Annotation	3	1	14	0	18
Répertoire	0	0	1	0	1
Langue	0	0	0	0	0
ATTEINTE À LA VIE PRIVÉE	17	45	141	16	219
Collecte	0	11	22	3	36
Conservation/Retrait	3	4	7	2	16
Usage & Communication	14	30	112	11	167
DÉLAIS	245	0	101	23	369
TOTAL	292	115	562	55	1,024

Si les ressources humaines et financières du Commissariat n'augmentent pas, le nombre de plaintes en souffrance grimpera à plus de 700 d'ici la fin de l'année en cours, soit à plus que le nombre total de plaintes ayant fait l'objet d'une enquête en 1987-1988.

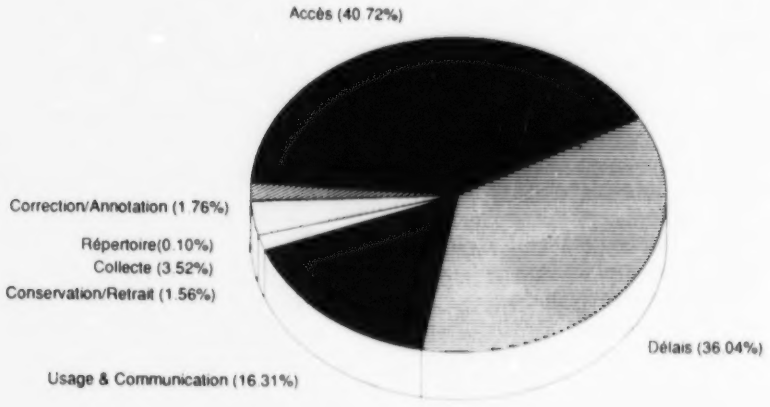
Bien que sa productivité se soit améliorée, le Commissariat n'a pas fermé plus de dossiers cette année que l'an dernier. Son efficience accrue a été plus que compensée par la baisse du nombre de plaintes concernant des retards, qui mobilisent moins de ressources que les autres, et par l'augmentation massive du nombre de plaintes concernant le code d'éthique sur les renseignements personnels, c'est-à-dire celles qui nécessitent les enquêtes les plus complexes et les plus longues.

Malheureusement, l'administration fédérale a rejeté les demandes du Commissariat, qui réclamait plus d'enquêteurs et plus de crédits de fonctionnement. Cette décision fera augmenter plus encore un arriéré déjà croissant, alourdira la charge des enquêteurs et prolongera la période d'attente des clients, qui veulent obtenir une décision sur leurs plaintes. Bref, le Commissariat lui-même risque désormais de devenir l'une des causes du problème.

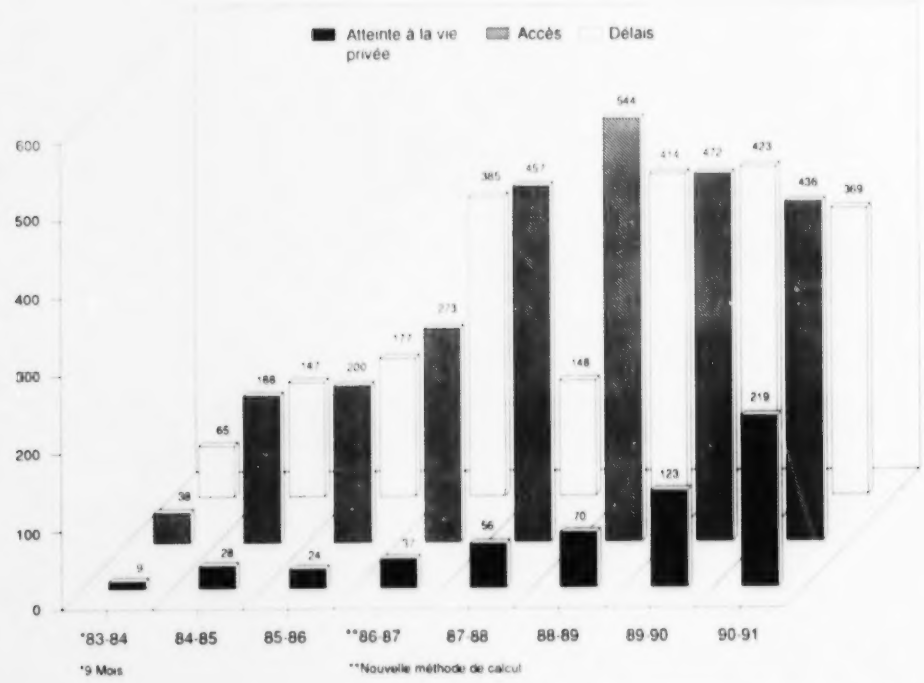
Origine des plaintes réglées

Terre-Neuve	0
Île-du-Prince-Édouard	8
Nouvelle-Écosse	41
Nouveau-Brunswick	36
Québec	148
Région de la Capitale nationale - Québec	6
Région de la Capitale nationale - Ontario	53
Ontario	407
Manitoba	66
Saskatchewan	33
Alberta	55
Colombie-Britannique	166
Territoires du Nord-Ouest	0
Yukon	5
Hors Canada	0
TOTAL	1,024

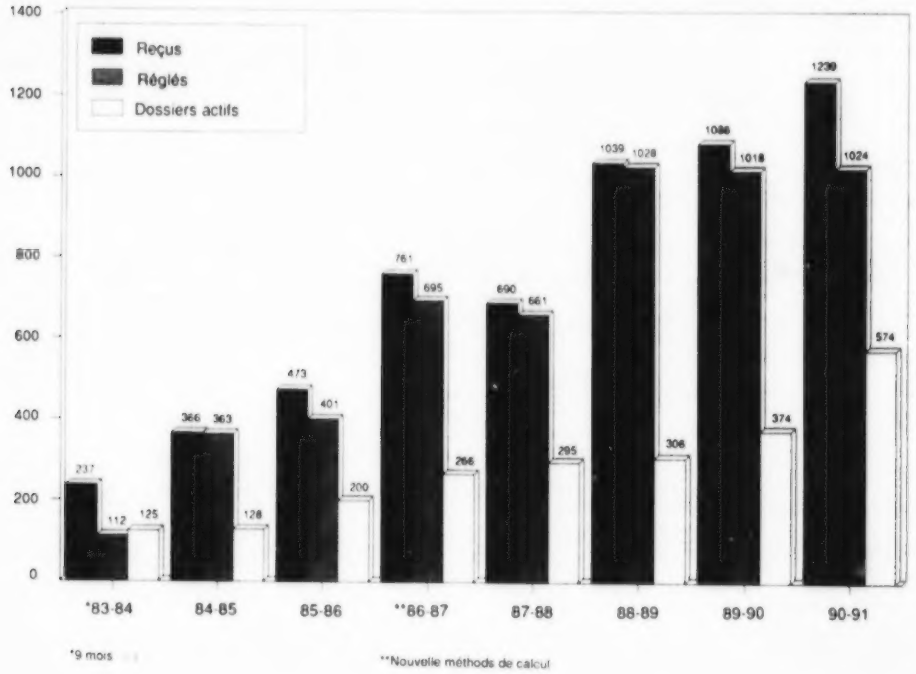
Plaintes réglées par motifs 1990-91



Plaintes réglées et motifs 1983-1991



Nombre de dossiers 1983-1991



*9 mois

**Nouvelle méthode de calcul

Plaintes Réglées par Institutions et Résultats

Ministère	NOMBRE	Résultats			
		Bien fondée	Bien fondée; résolue	Non fondée	Abandonnée
Anciens combattans Canada	5	3	0	2	0
Affaires extérieures Canada	7	3	0	3	1
Affaires indiennes et du Nord Canada	10	0	0	10	0
Agriculture Canada	11	2	1	8	0
Approvisionnements et Services Canada	3	0	2	1	0
Archives nationales du Canada	24	1	3	19	1
Bureau du Conseil privé	3	2	0	1	0
Commissariat aux langues officielles	1	0	0	1	0
Commission canadienne des droits de la personne	5	1	3	1	0
Commission de la fonction publique du Canada	2	0	0	2	0
Commission des plaintes du public contre la GRC	1	0	0	1	0
Commission des relations de travail dans la fonction publique	7	0	3	4	0
Commission nationale des libérations conditionnelles	20	2	5	13	0
Conseil du Trésor du Canada	1	0	0	0	1
Consommateurs et Sociétés	5	3	0	1	1
Défense nationale	84	34	8	31	11
Emploi et Immigration Canada	78	33	10	27	8
Environnement Canada	1	0	0	1	0
Finances Canada	1	0	0	1	0

Ministère	NOMBRE	Résultats			
		Bien fondée	Bien fondée; résolue	Non fondée	Abandonnée
Gendarmerie royale du Canada	78	2	3	66	7
Justice Canada	9	2	0	7	0
Monnaie royale canadienne	1	0	1	0	0
Musées nationaux du Canada	1	0	0	1	0
Pêches et Océans	6	1	3	1	1
Revenu Canada, Douanes et Accise	14	11	1	2	0
Revenu Canada, Impôt	71	43	0	28	0
Santé et Bien-être social Canada	34	16	3	15	0
Secrétariat d'État du Canada	3	2	0	1	0
Service canadien du renseignement de sécurité	83	6	9	67	1
Service correctionnel Canada	162	84	19	49	10
Société canadienne des postes	233	13	39	171	10
Société du crédit agricole Canada	1	0	0	1	0
Solliciteur général Canada	14	1	0	12	1
Statistique Canada	1	0	0	1	0
Transports Canada	42	27	2	12	1
Travail Canada	1	0	0	0	1
Voie maritime du Saint-Laurent	1	0	0	1	0
TOTAL	1,024	292	115	562	55

Dossiers

Les dossiers de l'Impôt ne doivent pas être utilisés par des admirateurs

Une journaliste a reçu à son domicile une lettre d'un admirateur qui est fonctionnaire fédéral. Elle a téléphoné au Commissariat pour savoir comment l'intéressé avait pu trouver son adresse personnelle. Elle ne voulait pas porter plainte, ni causer des difficultés à son admirateur, mais elle tenait à assurer sa sécurité et désirait savoir comment celui-ci s'était procuré son adresse.

Le Commissariat a eu beaucoup de mal à respecter les désirs de la journaliste tout en prenant des mesures pour que les fonctionnaires fédéraux évitent d'utiliser les dossiers gouvernementaux à des fins qu'on ne peut vraiment pas juger «compatibles» avec leurs fonctions, même avec la meilleure volonté du monde. L'agent enquêteur a remonté la filière jusqu'à Revenu Canada (Impôt).

Lorsqu'on lui a montré sa lettre, le fonctionnaire en cause a expliqué qu'il voulait simplement obtenir l'autographe de la journaliste. Il ne semblait pas poser le moindre danger pour elle. Soulagée, la journaliste a demandé que l'affaire soit abandonnée.

Toutefois, comme il avait appris que le fonctionnaire s'était servi de renseignements tirés des données de l'impôt, le Commissariat a dû en informer Revenu Canada, qui s'est donné un code d'éthique très strict à ce sujet et qui s'impose des mesures de sécurité radicales aux fins du traitement des dossiers des contribuables. Revenu Canada a fait enquête, conclu qu'il ne s'agissait pas d'un incident isolé et puni l'admirateur pour son inconduite.

Longs délais de traitement à Revenu Canada

La *Loi sur la protection des renseignements personnels* est maintenant en vigueur depuis huit ans, mais certains ministères continuent à faire fi des délais qu'elle impose.

Revenu Canada (Impôt), par exemple, témoigne parfois d'une souveraine indifférence quant au droit des demandeurs de recevoir les renseignements qu'ils réclament dans les délais prévus par la Loi. C'est vraiment paradoxal, puisqu'on sait avec quelle promptitude le fisc pénalise les contribuables qui produisent leur déclaration en retard...

Nous ne citerons qu'un exemple, celui d'une femme qui s'était rendue le 7 mai 1990 au bureau de l'impot de Vancouver pour demander où en était la demande qu'elle avait présentée en janvier afin de voir son dossier d'impôt sur le revenu. Revenu Canada n'avait pas trace de sa première demande, de sorte que la femme en a déposé une seconde. Le 26 juin, elle a fini par téléphoner au Commissariat pour se plaindre de n'avoir pas eu la moindre nouvelle à ce sujet.

Même après que le Commissariat se soit enquéri auprès de Revenu Canada (Impôt) au sujet du délai, ce dernier n'a pourtant procédé à la communication que le 13 août 1990, soit 96 jours après le dépôt de la seconde demande. Les ministères peuvent demander une prolongation du délai de 30 jours dans certaines circonstances, mais ils doivent en informer le demandeur, qui peut alors porter plainte si la prolongation du délai lui semble déraisonnable.

Revenu Canada n'a pas pu expliquer pourquoi il n'avait pas accusé réception de la demande de la plaignante, pourquoi il ne lui avait pas dit quand il lui fournirait le dossier et, en fin de compte, pourquoi il n'a pas respecté le délai.

Le Commissaire a jugé la plainte bien fondée.

La Cour fédérale ordonne au SCRS de répondre

Le Service canadien du renseignement de sécurité (SCRS) a informé un demandeur qu'il ne pouvait pas lui fournir les renseignements personnels que celui-ci réclamait dans les 30 jours prévus par la Loi.

Le délai était en partie imputable aux nombreuses demandes que le SCRS venait de recevoir, en raison semble-t-il d'un article paru dans le Toronto Star, ainsi qu'au fait qu'il lui fallait consulter d'autres parties avant de pouvoir communiquer les renseignements demandés.

Le demandeur a porté plainte au Commissaire et déclaré à l'agent enquêteur qu'il s'adresserait à la Cour fédérale si le SCRS ne lui donnait pas les renseignements dans le délai maximum de 60 jours autorisé par la Loi.

Le 61e jour, après avoir constaté que le SCRS n'avait toujours pas fini de traiter les dossiers du plaignant, le Commissaire conclu que la plainte était bien fondée, et il lui a confirmé sont droit de saisir la Cour fédérale de l'affaire. (Les plaignants ne peuvent pas se prévaloir de leur droit de recours en révision devant la Cour fédérale tant que l'enquête du Commissaire n'est pas terminée.)

Le plaignant a demandé à la Cour de délivrer un mandamus enjoignant au SCRS de produire les renseignements qu'il réclamait. Sa requête a été entendue 20 jours plus tard, et le juge a ordonné au SCRS de donner réponse à la demande du plaignant dans un délai d'un mois à partir de la date du jugement. Le SCRS a obtempéré.

Bien que le SCRS ait fini par produire les renseignements réclamés, l'audience et le délai supplémentaire d'un mois que la Cour lui a accordé ont prolongé de 50 jours la période d'attente du plaignant. La solution n'est vraiment pas satisfaisante; huit ans après la promulgation de la *Loi sur la protection des renseignements personnels*, il est inacceptable que les demandeurs doivent s'adresser à la Cour fédérale pour forcer une institution fédérale à leur communiquer les renseignements qu'ils réclament dans les délais prévus par la Loi.

Les militaires doivent avoir plus facilement accès à l'information lorsqu'ils présentent des griefs

Une plainte portée contre le ministère de la Défense nationale (MDN) l'a peut-être incité à modifier sa procédure de règlement des griefs des militaires. L'affaire a soulevé d'importantes questions sur l'accès des militaires aux renseignements factuels recueillis dans ce contexte par le service du contentieux du MDN.

Les avocats du MDN peuvent faire enquête sur les griefs des militaires afin de préparer des avis juridiques et de conseiller le chef de l'État-major de la Défense. Dans l'administration fédérale, ce sont normalement des agents des relations de travail (qui ne sont pas avocats) qui font enquête sur les griefs. La procédure utilisée dans le cas des militaires fait qu'une proportion accrue des documents pertinents est protégée par le secret professionnel qui lie l'avocat à son client.

Les problèmes que cela cause ont sauté aux yeux du Commissaire quand un officier s'est plaint que le MDN lui avait refusé une grande partie des renseignements contenus dans son dossier de grief en invoquant le secret professionnel ou en disant qu'il s'agissait de renseignements personnels concernant des tiers. L'agent enquêteur a confirmé que le MDN s'était réclamé de la relation privilégiée entre l'avocat et son client pour tous les documents obtenus ou rédigés par son service du contentieux pendant l'enquête sur le grief. Le MDN a soutenu que les documents devaient être protégés puisque ses avocats avaient préparé le dossier dans le but exprès de rédiger un avis juridique et des recommandations pour le haut commandement.

Le Commissaire a contesté une interprétation aussi large du secret professionnel qui lie l'avocat à son client, en déclarant à la fois injuste et contraire à l'intention du législateur qu'on invoque cette protection pour éviter de communiquer des faits et des témoignages recueillis au cours de l'enquête. Il a proposé au MDN de se prévaloir de sa latitude pour communiquer plus de renseignements au plaignant. Le MDN a accepté de réévaluer sa position; l'officier a reçu 10 autres pages de texte, comprenant notamment les déclarations des témoins.

Par ailleurs, le Commissaire a admis que le reste des documents qui n'avaient pas été communiqués au plaignant contenaient des renseignements personnels sur des tiers, et que le MDN avait donc eu raison de ne pas les divulguer. Depuis, le MDN a révisé sa procédure de règlement des griefs des militaires, et communique désormais à ceux-ci tous les documents (à quelques rares exceptions près) dont il doit être tenu compte à l'arbitrage de leurs griefs.

Il n'est pas possible de refuser de divulguer des renseignements à un demandeur s'ils doivent être communiqués à son médecin

Un ancien militaire a porté plainte au Commissaire quand les Archives nationales ont refusé de lui communiquer certaines parties de ses dossiers médicaux datant de l'époque où il était militaire, en invoquant l'article 28 de la Loi pour dire que l'examen d'une évaluation de son état de santé mentale faite 25 ans auparavant le desservirait. Par contre, les Archives étaient disposées, s'il y consentait par écrit, à divulguer les renseignements demandés à son médecin, qui aurait pu lui expliquer l'évaluation en question.

La réglementation sur la protection des renseignements personnels autorise les ministères et organismes à obliger les demandeurs à n'examiner leurs dossiers médicaux qu'en présence d'un médecin qualifié ou d'un psychologue capable de leur expliquer l'information que ceux-ci renferment.

Le plaignant soutenait qu'il connaissait la teneur de son évaluation et qu'il n'avait pas besoin d'explications.

Le Commissaire a jugé que, si les Archives étaient d'avis qu'il serait à l'avantage du demandeur de ne pas voir le dossier en question, elles auraient dû refuser catégoriquement de le divulguer. Par contre, si elles étaient disposées à le divulguer, même par l'intermédiaire de son médecin, il était illogique qu'elles prétendent que sa divulgation allait desservir le plaignant.

Le Commissaire s'est aussi demandé pourquoi les Archives voulaient refuser de communiquer le dossier au plaignant en se fondant sur l'évaluation qu'un psychiatre retenu à cette fin avait faite du dossier quand le plaignant avait présenté des demandes analogues, en 1985 et en 1990. Le Commissaire a conclu que cette évaluation psychiatrique n'était pas digne de foi, étant donné qu'elle n'était fondée que sur un examen de dossiers médicaux datant de 25 ans et qu'elle ne tenait pas compte de l'état émotionnel actuel du plaignant.

Les renseignements réclamés ont été divulgués après que le Commissaire eut conclu que le plaignant avait le droit de voir son dossier. Qui plus est, les Archives nationales ont accepté de modifier leur procédure de traitement des renseignements médicaux de nature délicate. À l'avenir, elles refuseront tout simplement de divulguer ces renseignements, ou les divulgueront directement au demandeur ou à son médecin.

Les témoignages doivent être divulgués à la fin des enquêtes

Une dame qui avait porté plainte à la Commission canadienne des droits de la personne (CCDP) dans un cas de discrimination avait demandé à voir les renseignements contenus dans son dossier de plainte. Quand la CCDP a refusé de lui communiquer certains de ces renseignements, elle s'est plainte au Commissaire à la protection de la vie privée.

La CCDP avait refusé de divulguer à la plaignante les adresses et numéros de téléphone d'autres personnes, ainsi que les déclarations des témoins. Le Commissaire a reconnu que la CCDP avait eu raison de refuser de divulguer les renseignements personnels concernant des tiers, mais il a contesté la non-divulgation des témoignages une fois l'enquête terminée.

En général, le Commissaire est d'avis que les témoignages ne devraient pas être divulgués tant que l'enquête est en cours, étant donné que leur divulgation risquerait d'influer sur ses résultats. En l'occurrence, toutefois, l'enquête était déjà terminée. Le Commissaire a donc demandé à la CCDP ce qu'on risquait si la plaignante était autorisée à consulter les témoignages.

La CCDP a été incapable de prouver que la divulgation des témoignages risquait vraiment de nuire à l'enquête en question ou à des enquêtes ultérieures. Néanmoins, le Commissaire a dû beaucoup insister avant qu'elle finisse par accepter de divulguer les témoignages à la plaignante.

Comme les renseignements demandés avaient d'abord été refusés, le Commissaire a jugé la plainte bien fondée, mais résolue.

Revenu Canada peut avoir accès aux relevés des dépenses personnelles des contribuables

Une Ontarienne qui avait des difficultés à payer ses arrérages d'impôt fédéral a porté plainte contre Revenu Canada (Impôt). Elle s'est fâchée quand un agent du fisc a insisté pour examiner ses dépenses personnelles afin d'évaluer sa capacité de payer, en invoquant la Loi de l'impôt sur le revenu. La contribuable jugeait que le procédé était abusif et qu'il violait sa vie privée.

L'article 4 de la *Loi sur la protection des renseignements personnels* dispose que : «Les seuls renseignements personnels que peut recueillir une institution fédérale sont ceux qui ont un lien direct avec ses programmes ou ses activités.» Par conséquent, les fonctionnaires fédéraux ne peuvent recueillir que les renseignements personnels dont ils ont manifestement besoin pour administrer leurs programmes.

Revenu Canada a expliqué qu'il est chargé de percevoir l'impôt sur le revenu des particuliers aux fins de l'application de la *Loi de l'impôt sur le revenu*. Sa procédure de perception est conçue de façon que cette Loi s'applique également à tous les contribuables, tout en lui permettant de tenir compte de la situation financière de chacun. Pour être juste avec la majorité des citoyens, qui payent sans tarder, la politique est ferme à l'endroit de ceux qui se font tirer l'oreille.

Le Commissaire a analysé la politique de perception de Revenu Canada, et il a reconnu que l'agent de perception avait besoin d'examiner les dépenses personnelles de la contribuable. Par conséquent, celle-ci était tenue par la *Loi de l'impôt sur le revenu* de fournir ce genre de renseignements. Le Commissaire a donc jugé que Revenu Canada avait respecté les dispositions sur la collecte de renseignements de la *Loi sur la protection des renseignements personnels* et conclu que la plainte n'était pas fondée.

La politique d'embauche doit concilier l'équité et le droit à la vie privée

Une plainte portée contre Emploi et Immigration Canada (EIC) a révélé à quel point il peut être difficile d'assurer la transparence des méthodes d'embauchage sans violer l'intimité des candidats.

Deux candidates qui avaient gagné un concours interne d'EIC ont porté plainte au Commissariat en disant qu'une agente de dotation avait communiqué leurs évaluations de rendement et les noms des personnes qui devaient leur fournir des références à une autre fonctionnaire qui en appelait des résultats du concours. Cette fonctionnaire avait par la suite divulgué le tout à l'ensemble du personnel du bureau des deux candidates sélectionnées.

Conformément à la politique sur les appels de la Commission de la fonction publique, les ministères et organismes ne sont tenus de divulguer que les renseignements personnels directement pertinents concernant les candidats sélectionnés. En l'occurrence, on s'était servi des évaluations de rendement pendant la procédure de dotation, mais elles n'avaient pas été mentionnées pendant l'appel et il n'en avait pas été tenu compte dans la décision d'appel. Elles n'étaient donc pas pertinentes. Leur divulgation a entraîné une grave violation du droit à la vie privée des plaignants, même si, au départ, l'agent de dotation a peut-être simplement péché par souci exagéré d'équité.

EIC a rappelé à toutes ses divisions du personnel la politique de divulgation des renseignements de ce genre. En outre, elle distribuera des lignes directrices plus détaillées pour faciliter le travail des agents de dotation, pris entre l'enclume de l'équité dans leur travail et le marteau de la protection de la vie privée des candidats.

Divulgation au pays d'origine d'une demande de statut de réfugié

Le plaignant, qui avait demandé le statut de réfugié, a reproché à un agent d'Emploi et Immigration Canada d'avoir communiqué des renseignements personnels à son sujet aux États-unis sans son autorisation.

Au cours de l'audition de sa demande de statut de réfugié, on avait constaté que le plaignant avait été déclaré coupable d'une infraction criminelle alors qu'il se trouvait aux États-Unis, mais qu'il ne s'était pas présenté pour se faire imposer sa peine.

Le plaignant avait déclaré que cette situation n'équivalait pas à une condamnation au pénal dans l'État en question. L'agent d'immigration a alors écrit au Greffier de la Première Cour de circuit de l'État pour obtenir son opinion à ce sujet. Ce faisant, il a divulgué le fait que le plaignant avait demandé le statut de réfugié au Canada. La Cour de l'État a confirmé que la déclaration de culpabilité équivalait à une condamnation.

Comme l'un des objectifs de la *Loi sur l'immigration* est de promouvoir l'ordre et la justice à l'échelle internationale, en n'acceptant pas sur le territoire canadien des personnes susceptibles de se livrer à des activités criminelles, le Commissaire a décidé qu'il s'agissait d'une utilisation des renseignements compatible avec les fins auxquelles ceux-ci avaient été recueillis, et que, par conséquent, le geste de l'agent d'immigration était justifié. Il a donc décidé que la plainte était non fondée.

Une demande de renseignements prématurée : l'affaire du dépôt direct

Quand l'administration fédérale a annoncé qu'elle cesserait de payer les fonctionnaires par chèque à partir du 1er avril 1991 et qu'elle commencerait alors à déposer le montant correspondant directement dans leur compte bancaire, plusieurs fonctionnaires ont communiqué avec le Commissariat pour savoir s'ils étaient tenus de divulguer leur numéro de compte à l'employeur.

Le Commissaire a fait enquêter lorsqu'il a été saisi d'une plainte en bonne et due forme d'un fonctionnaire de Transports Canada, qui s'était fait demander ce renseignement par le Ministère. Il n'était vraiment pas content.

Le Conseil du Trésor, autrement dit l'employeur, peut-il obliger les fonctionnaires à leur indiquer leur succursale et le numéro de leur compte bancaire aux fins du dépôt direct? La Loi l'autorise-t-elle à recueillir ces renseignements?

Le Commissaire a conclu que l'employeur a effectivement le droit de décider comment payer ses fonctionnaires. Par conséquent, il ne violerait pas la *Loi sur la protection des renseignements personnels* en recueillant l'information qu'il lui faut pour administrer la paye.

Il restait encore à savoir comment l'employeur allait réagir dans le cas des fonctionnaires qui refuseraient de lui fournir ces renseignements. Allait-il donner leur nom, leur adresse et leur numéro d'assurance sociale à une banque, en demandant à celle-ci de leur ouvrir un compte sans leur consentement?

Le personnel du Commissariat a eu plusieurs rencontres avec des représentants du Conseil du Trésor, qui ont déclaré que la participation au régime de dépôt direct était encore volontaire, et que Transports Canada avait tout simplement été trop pressé de commencer. On n'avait recueilli des renseignements qu'auprès des personnes qui avaient décidé d'adhérer au régime. Cela dit, l'employeur était conscient du problème qu'allaient poser les récalcitrants.

Néanmoins, compte tenu de ce que le Président du Conseil du Trésor avait annoncé en décembre 1989, il semblait bien que la fonction publique s'orientait vers un régime de dépôt direct obligatoire. Le Commissaire a donc décidé de garder le dossier ouvert jusqu'à ce que la politique soit plus claire.

Le 15 décembre 1990, l'employeur a annoncé que la participation au régime de dépôt direct demeurerait volontaire. Les plaignants ne seraient pas tenus de divulguer l'information nécessaire, et l'employeur n'ouvrirait pas de compte en leur nom. Le Commissaire a conclu que la plainte n'était pas fondée.

La Commission des relations de travail dans la fonction publique conserve désormais ses pièces pendant deux ans

Bien que le Règlement sur la protection des renseignements personnels oblige les organismes gouvernementaux à les conserver au moins deux ans, une plainte a révélé que la Commission des relations de travail dans la fonction publique (CRTFP) ne conservait ses pièces que trois mois avant de les faire détruire ou de les renvoyer à la partie qui les avait déposées.

Le Règlement prévoit une période de conservation de deux ans pour que les citoyens aient l'occasion de consulter les documents qui les intéressent.

Une femme s'est plainte qu'on avait porté atteinte à ses droits de protection des renseignements personnels parce que la CRTFP avait détruit des pièces bien avant l'expiration de la période de deux ans.

La CRTFP a expliqué à l'agent enquêteur qu'elle n'avait pas l'espace nécessaire pour conserver toutes les pièces, qui peuvent comprendre aussi bien des volumes entiers de documents que des articles aussi hétéroclites qu'un bâton de baseball brisé, des poubelles, voire une corde de pendu! La Commission a de plus souligné que toutes les parties aux audiences reçoivent copie des pièces, de sorte que rien n'est détruit qu'elles n'aient déjà reçu.

Il n'empêche que le Règlement est clair. Le Commissaire a conclu que la CRTFP doit conserver les pièces contenant des renseignements personnels au moins deux ans après la dernière mesure administrative prise à leur égard. La Commission a accepté cette conclusion, et le Commissaire a jugé la plainte résolue.

Les renseignements personnels divulgués devraient être corrects

Un employé de longue date de la Société canadienne des postes (SCP) s'est plaint au Commissaire que son employeur avait communiqué des renseignements médicaux incorrects à son sujet à la Commission des accidents du travail, afin de lui faire refuser des prestations auxquelles il avait droit.

La SCP avait déclaré à la Commission des accidents du travail que le plaignant n'avait pas droit à ces prestations parce que sa blessure était imputable à des troubles chroniques. La superviseure du plaignant a déclaré que c'était le plaignant lui-même qui lui avait déclaré cela, et qu'elle n'avait fait que répéter des faits qu'elle croyait pertinents dans le contexte de sa réclamation.

Pour sa part, le plaignant a nié souffrir de troubles chroniques, et ses dires ont été confirmés lorsqu'il s'est fait examiner par un spécialiste. Il a aussi nié avoir jamais dit à quiconque, et surtout pas à sa superviseure, qu'il souffrait d'une affection de ce genre.

L'agent enquêteur a constaté un facteur qui peut avoir envenimé la situation. En effet, la SCP ne lâche pas facilement le morceau dans le contexte des accidents du travail, dans le but de limiter les frais le plus possible. Elle prétend d'ailleurs être tenue de divulguer à la Commission des accidents du travail tout renseignement susceptible de mettre en doute la validité des réclamations.

La *Loi sur la protection des renseignements personnels* dispose que les renseignements de cette nature utilisés à des fins administratives doivent être aussi exacts, à jour et aussi complets que possible. Dans ce cas-ci, rien ne permet de croire que la superviseure ait fait le moindre effort pour vérifier la validité des renseignements médicaux qu'elle avait communiqués à la Commission des accidents du travail.

Après avoir longtemps discutaillé, la SCP a fini par accepter de déclarer à la Commission des accidents du travail qu'elle n'avait aucune preuve de sa prétention que le plaignant souffrait des troubles en question.

Le Commissaire a jugé la plainte bien fondée et résolue.

La liste des titulaires de permis ne doit pas être utilisée pour des enquêtes

Lorsqu'un dirigeant d'une compagnie aérienne a téléphoné au Commissariat au sujet d'une enquête de Transports Canada sur l'utilisation de médicaments et de drogues, le Commissaire a décidé d'enquêter de sa propre initiative.

Le correspondant du Commissaire avait commencé à s'inquiéter quand une entreprise de recherche sur les marchés lui avait demandé le nom, l'adresse et le numéro de téléphone de ses employés. L'entreprise en question lui avait dit qu'elle avait été chargée par Transports Canada d'une enquête sur l'utilisation de médicaments, de drogues et d'autres substances dans le secteur des transports, et qu'elle avait besoin de ces renseignements personnels pour choisir au hasard les personnes qui allaient participer à l'enquête.

Il s'est avéré que l'enquête en question était un important volet de l'étude que Transports Canada avait amorcée en vue de déterminer dans quelle mesure la consommation de médicaments, de drogues et d'alcool par les employés du secteur des transports représentait un danger pour la sécurité dans ce domaine. Les répondants devaient remplir un questionnaire sur leur consommation d'alcool, de médicaments (sur ordonnance et en vente libre), de drogues, de même que sur les conditions existant à leur lieu de travail qui pouvaient influer sur leur utilisation de ces substances.

À cet égard, il fallait se poser deux questions en ce qui concerne la protection de la vie privée, à savoir si les règles de collecte des renseignements personnels avaient été respectées pendant l'enquête, et si Transports Canada avait respecté les dispositions sur l'utilisation et la divulgation de ces renseignements prévues par la *Loi sur la protection des renseignements personnels*.

Ces restrictions en matière d'utilisation et de divulgation obligent les ministères et organismes fédéraux à recueillir seulement les renseignements personnels ayant un lien direct avec leurs programmes ou leurs activités. En outre, ces renseignements doivent être recueillis directement auprès de la personne intéressée, chaque fois que possible, à moins que cela n'amène les responsables à recueillir des renseignements incorrects, contrarie les fins auxquelles ceux-ci sont destinés ou en compromette l'usage. En outre, la personne intéressée doit être informée des fins auxquelles les renseignements recueillis sont destinés.

L'enquête a révélé que les questionnaires ne contenaient pas de renseignements personnels permettant de les relier à quelqu'un de précis. Bref, étant donné que les répondants ne pouvaient pas être identifiés, les renseignements recueillis n'étaient pas réellement «personnels», de sorte que leur collecte ne constituait pas une infraction à la *Loi sur la protection des renseignements personnels*.

Toutefois, il était clair que Transports Canada avait compilé la liste de certains des participants à l'enquête à partir de renseignements personnels recueillis à d'autres fins, dont aucune ne comprenait leur divulgation à des organismes de recherche. Dans la plupart des secteurs, Transports Canada n'avait donné à l'entreprise chargée de l'enquête que le nom et le numéro de téléphone des participants éventuels, mais, dans le cas du personnel aéroportuaire, on avait utilisé une liste d'employés titulaires de permis de conduire des véhicules côté piste; comme la divulgation de leurs noms n'était pas compatible avec les fins auxquelles ils avaient été recueillis, elle n'était pas justifiée.

L'agent enquêteur a aussi constaté que les responsables de l'enquête avaient commencé à recueillir des renseignements avant même d'avoir signé des contrats écrits. Or, les projets de contrats étaient muets sur les principes de collecte de renseignements prévus par la Loi. Par conséquent, des représentants du Commissariat, d'Approvisionnements et Services (l'organisme qui passait les marchés d'enquête) et de Transports Canada se sont réunis pour fixer des règles ayant pour objet d'assurer que tous les marchés conclus à des fins de collecte de renseignements personnels contiendront des clauses normalisées sur la collecte, la conservation, l'utilisation, la divulgation et le retrait de ces renseignements, de façon à être conformes à la Loi.

Le Commissaire a par ailleurs recommandé à Transports Canada d'obtenir le consentement des personnes visées avant d'envisager toute utilisation ultérieure des renseignements personnels les concernant qui ne serait pas compatible avec les fins auxquelles ceux-ci auraient été recueillis à l'origine.

Aviser le Commissaire

Cette année, le Commissariat a reçu 50 préavis d'organismes gouvernementaux qui allaient divulguer des renseignements personnels pour des raisons «d'intérêt public» ou à l'avantage des personnes concernées. Ces divulgations allaient de la confirmation de la citoyenneté des intéressés, afin que ceux-ci puissent toucher des pensions ou des indemnités, jusqu'à des rapports détaillés sur des évasions de pénitenciers fédéraux. En fait, les incidents impliquant des détenus sont désormais une constante dans les cas de préavis (voir la page 28 pour plus de détails).

Voici quelques exemples d'autres préavis pour des raisons d'intérêt public.

Le MDN divulgue des détails tirés d'un dossier d'attestation de sécurité

Le ministère de la Défense nationale (MDN) a avisé le Commissaire de son intention de divulguer à un fonctionnaire des renseignements normalement jugés confidentiels, tirés de son dossier d'attestation de sécurité.

Le personnel du MDN était en train d'étudier la demande que l'intéressé avait présentée pour voir son dossier lorsqu'il a appris que la sûreté provinciale avait porté des accusations de nature criminelle contre lui, notamment dans un cas d'agression sexuelle contre une ancienne fonctionnaire. Le dossier d'attestation de sécurité du demandeur contenait un compte rendu de l'interrogatoire auquel la fonctionnaire plaignante avait été soumise par la police militaire, et durant lequel elle avait donné des détails sur sa longue liaison sexuelle avec l'intéressé. Elle avait fait clairement comprendre à la police militaire que cette liaison était désirée par les deux parties.

Comme la *Loi sur la protection des renseignements personnels* autorise les organismes d'enquête (y compris la police militaire) à protéger les sources interrogées au cours des enquêtes effectuées en vue d'accorder des attestations de sécurité, le MDN aurait normalement refusé de divulguer les commentaires de la fonctionnaire en question, car ils la concernaient tout autant que l'intéressé, et il aurait été virtuellement impossible de ne tirer du dossier que les renseignement concernant ce dernier; en outre, la source des renseignements aurait été évidente.

Le MDN était en proie à un dilemme en ce qu'il avait accepté de traiter confidentiellement des renseignements qui semblaient contredire les accusations portées contre l'intéressé par l'ancienne fonctionnaire. Comme l'intéressé ne savait peut-être pas que ces renseignements figuraient dans son dossier, il aurait pu être privé de détails d'une importance cruciale pour sa défense. Le MDN a conclu qu'il était nécessaire, pour des raisons d'intérêt public, de lui fournir ces renseignements avant le début du procès.

Le Commissaire a informé l'ancienne fonctionnaire de la divulgation.

Une femme reçoit des détails sur les circonstances entourant le décès de son fils à l'étranger

Une femme a demandé à la GRC et aux Affaires extérieures de lui communiquer les renseignements qu'elles détenaient sur les circonstances entourant le décès de son fils en Thaïlande. La GRC et les Affaires extérieures estimaient que l'enquête menée par les autorités thaïlandaises avait été concluante, et un pathologiste canadien avait confirmé les résultats de l'autopsie pratiquée sur place, mais la mère se posait encore des questions, de sorte que la GRC voulait lui communiquer 21 des pages de son rapport d'enquête, en n'en retirant que quelques renseignements concernant d'autres personnes. Pour leur part, les Affaires extérieures étaient disposées à lui fournir des documents tirés des dossiers conservés dans deux de ses ambassades à l'étranger ainsi qu'à son administration centrale, à Ottawa.

Normalement, *la Loi sur la protection des renseignements personnels* interdirait la divulgation de ces renseignements, même à la mère du défunt. Toutefois, les deux organismes en cause jugeaient qu'il était préférable, pour des raisons d'intérêt public, de lui communiquer le rapport afin qu'elle puisse poursuivre ses démarches en Thaïlande, et afin aussi de la rassurer, si possible. Le Commissaire s'est dit d'accord.

Un demandeur cherchait à obtenir une liste de dividendes non réclamés

Un demandeur a invoqué la *Loi sur l'accès à l'information* pour obtenir de Consommateurs et Sociétés Canada (CSC) des listes de dividendes non réclamés en vertu de trois lois, la *Loi sur la faillite*, la *Loi sur les sociétés par actions* et la *Loi sur les liquidations*. Il voulait retracer les créanciers.

CSC a avisé le Commissaire de son intention de divulguer les listes demandées, parce que ce serait à l'avantage des individus concernés (sous-alinéa 8(2)m)(ii)). Le Commissaire s'est dit d'accord, mais en ajoutant qu'il ne cessait pas d'éprouver un certain malaise quant à l'opportunité d'une telle divulgation. Il a souligné que, si les institutions gouvernementales sont capables de retracer sans trop de mal les personnes auxquelles elles doivent de l'argent, elles devraient le faire. Il a conclu qu'il ne lui semblait vraiment pas idéal de divulguer des renseignements personnels sans le consentement des intéressés, pour permettre à des tiers de localiser des créanciers, sans doute moyennant rétribution.

Un piètre coup de filet pour Revenu Canada

Pêches et Océans Canada a avisé le Commissaire de son intention de fournir au Bureau des communications (TPS) de Revenu Canada une liste d'adresses postales de pêcheurs commerciaux. Le Bureau de la TPS voulait envoyer à ces pêcheurs une brochure d'information leur expliquant comment facturer, consigner, calculer et verser la taxe. Revenu Canada n'avait pas d'autres moyens de communiquer avec les pêcheurs, de sorte que Pêches et Océans a conclu qu'il était manifestement à l'avantage de ces derniers de recevoir le document en question. Le Commissaire n'en était pas si sûr. En effet, la loi portant création de la TPS n'avait pas encore été adoptée, et, bien que la divulgation de la liste aurait pu être utile, il n'était pas convaincu qu'elle allait présenter un avantage certain pour les pêcheurs. Néanmoins, il a déclaré à Pêches et Océans qu'il ne s'opposait pas à son envoi de la brochure pour le compte de Revenu Canada.

Pêches et Océans n'a pas jugé avoir des raisons d'intérêt public suffisantes pour se charger de l'envoi postal de la brochure sur la TPS, en décidant toutefois de fournir à Revenu Canada une liste des associations de pêcheurs.

Les noms des membres du conseil d'administration ne sont pas des renseignements «personnels»

Le Centre de recherches pour le développement international (CRDI) a informé le Commissaire qu'il divulguerait les noms des membres de son conseil d'administration qui avaient assisté à une de ses réunions, à Bangkok, en Thaïlande. Le Centre avait donné à un journaliste (qui en avait fait la demande en vertu de la *Loi sur l'accès à l'information*) un relevé des notes de frais de ces personnes, mais pas leurs noms. Le journaliste s'était plaint au Commissaire à l'information, qui avait recommandé au CRDI de divulguer les renseignements demandés.

Après avoir discuté de l'avis qu'il avait reçu avec le personnel du CRDI, le Commissaire à la protection de la vie privée a souscrit au raisonnement du Commissaire à l'information, qui estimait que les membres du Conseil d'administration du Centre faisaient partie de son personnel de direction et que, par conséquent, leurs notes de frais ne seraient pas normalement considérées comme des «renseignements personnels». Toutefois, en préparant les documents réclamés par le journaliste, le CRDI y avait fait figurer plus de détails que nécessaire (les plats commandés, les numéros d'assurance sociale et le genre de cartes de crédit des membres, voire le numéro de carte American Express de l'un d'eux).

Fournir des détails pareils va au-delà des exigences de l'imputabilité. Après avoir fait cette erreur, le CRDI ne pouvait plus refuser de divulguer les noms des intéressés. Le Commissaire a donc accepté qu'il le fasse, comme il l'en avait avisé, et le CRDI a informé les membres de son conseil d'administration de la divulgation.

Politique et recherche

Couplage de données informatiques

Le traitement électronique des données présente des risques particuliers pour la vie privée. Ainsi, le couplage incontrôlé de fichiers informatiques pourrait aboutir à la production de dossiers détaillés sur tout le monde, ce qui tournerait en ridicule les restrictions imposées par la Loi en matière de collecte des renseignements.

Pour parer à ce risque, l'administration fédérale s'est donnée il y a un peu plus d'un an une politique de couplage des données obligeant les ministères et organismes à soumettre au Commissaire à la protection de la vie privée des propositions détaillées au moins 60 jours avant de commencer à établir une liaison entre bases de données. La politique freinera le couplage incontrôlé des données en permettant à un tiers, le Commissaire à la vie privée, d'évaluer leurs propositions en toute indépendance, à partir d'un ensemble de critères dûment approuvés. Le Commissaire jouera aussi le rôle de défenseur de tous ceux qui pourraient être affectés par les résultats.

Malheureusement, certains ministères et organismes semblent avoir l'impression que le Commissaire doit simplement se contenter d'approuver leurs projets après en avoir été informé à la dernière minute. La politique du Conseil du Trésor est pourtant claire, et le Commissaire fait ses évaluations avec sérieux. Ceux qui le préviennent quand leur système est déjà prêt à démarrer ne feront que causer des retards frustrants pour tous les intéressés.

Cette année, le personnel du Commissariat a étudié 11 propositions soumises en vertu de la politique. Dans les pages qui suivent, nous allons donner une description succincte de chacune d'entre elles, avec un résumé de nos conclusions. Pour obtenir plus de détails - ou des conseils sur la façon de préparer des propositions - il suffit de nous téléphoner.

Couplage des fichiers du Programme d'aide à l'adaptation d'Emploi et Immigration Canada avec ceux du bien-être social de la Région métropolitaine de Toronto

Des représentants des autorités fédérales et ontariennes ainsi que de la Région métropolitaine de Toronto ont formé un comité pour résoudre certains des problèmes résultant du nombre croissant de personnes de cette Région qui ont réclamé le statut de réfugié et qui touchent des prestations de bien-être social.

Il s'agit notamment de savoir si ces gens reçoivent une aide financière du Programme d'aide à l'adaptation d'Emploi et Immigration Canada, qui donne de l'argent aux réfugiés jusqu'à ce que ceux-ci aient des revenus suffisants pour subvenir à leurs besoins (ou pour une période d'un an, selon la première des deux éventualités). Les réfugiés qui bénéficient de l'aide financière du Programme ne peuvent pas toucher de prestations de bien-être social.

Les membres du comité craignaient que les deux programmes reçoivent des demandes frauduleuses, faute d'une forme quelconque de vérification. Ils ont donc convenus qu'EIC et la Région métropolitaine de Toronto coupleraient leurs données pour éliminer ce risque.

Au début, EIC a déclaré que le couplage était «compatible» avec les fins auxquelles les renseignements avaient été recueillis, sans donner guère plus d'explications au Commissaire. Toutefois, après de longues consultations, les responsables ont donné la raison d'être du couplage et fourni des arguments juridiques pour le justifier.

Le Commissaire s'est dit satisfait, mais il a demandé à EIC de suivre l'exemple de la Région métropolitaine de Toronto, en disant aux demandeurs que leur admissibilité devait être vérifiée par les autorités. Il lui a en outre demandé d'ajouter un avis et une déclaration de consentement à ses formules de demande, ainsi que de vérifier si le couplage réduisait suffisamment le nombre de demandes frauduleuses pour en valoir la peine. EIC a accepté.

Le projet INFONNEL des Affaires extérieures

Dans le rapport annuel de l'an dernier, nous avions dit que les Affaires extérieures avaient demandé au Commissariat d'étudier le système de gestion du personnel dont elles envisageaient de se doter, et qui aurait consisté à fusionner de petites bases de données pour en faire un système intégré offrant des possibilités de traitement plus étendues. Le système devait permettre à la direction de prévoir, suivre et enregistrer toutes les mesures prises dans le domaine du personnel.

Le personnel du Commissariat craignait que les applications rendues possibles par le degré d'intégration envisagé excèdent les limites approuvées par le Conseil du Trésor pour ce genre de base de données; de plus, la proposition ne contenait pas suffisamment de détails sur les caractéristiques de sécurité du système. Bref, sa conception ne satisfaisait pas aux exigences de la *Loi sur la protection des renseignements personnels* ou de la politique de sécurité gouvernementale.

Les difficultés n'ont pas pu être résolues grâce aux documents de suivi et aux discussions qui ont eu lieu par la suite, de sorte que les vérificateurs du Commissariat devront analyser le système.

Système de sécurité des renseignements d'Agriculture Canada

Agriculture Canada a consulté le Commissariat au sujet de son projet de transférer certains renseignements personnels sur ses fonctionnaires de son système des ressources humaines à un système assurant la sécurité des renseignements.

Le Ministère s'est adressé au Commissariat dès les premières étapes de son projet de couplage d'épuration. (L'épuration sert à vérifier ou mettre à jour une base de données.) Dans sa proposition, il a expliqué pourquoi il estimait le transfert compatible avec les fins auxquelles les renseignements avaient été recueillis. Il comptait agir vite pour modifier les descriptions de la banque de données afin de refléter le changement. Comme Agriculture Canada avait parfaitement respecté la politique, l'examen de sa proposition s'est fait rapidement ... et sans douleur.

Répertoire des balises de localisation individuelles

Le Commissariat a approuvé le projet du ministère des Communications de mettre en place un nouveau système contenant des données sur les détenteurs de «balises de localisation individuelles». Ces appareils sont de petits émetteurs portatifs dont les campeurs, canotiers et randonneurs se munissent et qu'ils actionnent en cas d'urgence. Leur signal radio facilite la recherche et le sauvetage.

Les Communications voulaient constituer un répertoire auquel les intéressés se seraient inscrits volontairement, et qui aurait contenu des renseignements comme leurs nom, adresse, type de véhicule et d'activité (terrestre, maritime ou aérienne), ainsi que le nom du parent à contacter en cas d'urgence. Le répertoire aurait été mis à la disposition du MDN et de la GRC, et il aurait aussi été couplé avec le système conjoint de renseignements utilisés pour la recherche et le sauvetage du MDN et de Transports Canada.

L'inscription au répertoire sera purement volontaire et les renseignements seront utilisés uniquement aux fins pour lesquelles ils auront été recueillis. Les personnes inscrites devront signer une formule de consentement, et elles seront informées de toute divulgation éventuelle. Enfin, toutes les données personnelles contenues dans le répertoire seront stockées dans une nouvelle banque de données personnelles figurant dans le guide **InfoSource**.

Nouveau service de counselling professionnel pour les cadres

Le Commissariat ne s'est pas non plus fait tirer l'oreille pour approuver la proposition de la Commission de la fonction publique (CFP) de constituer un répertoire à l'intention de son nouveau service de counselling confidentiel, qui doit aider les cadres à améliorer leurs aptitudes.

Personne n'est tenu de se prévaloir de ce service, qui découle d'ailleurs du mandat de la CFP. Les participants lui fournissent directement les renseignements demandés et il leur dit comment il compte les utiliser. La CFP constituera une banque réservée aux données recueillies à cette fin.

La TPS et le NAS

L'avis que Revenu Canada a envoyé au Commissariat au sujet du couplage de données rendu nécessaire par la mise en vigueur de la TPS ne s'est pas fait sans accrocs.

Au début de 1990, le ministre du Revenu a informé le Commissaire que la mise en vigueur de la TPS nécessiterait un certain couplage de données et qu'il se servirait des numéros d'assurance sociale des contribuables pour enregistrer et les particuliers, et les entreprises individuelles. Il a assuré le Commissaire que Revenu Canada prenait très au sérieux le droit à la vie privée de ses clients, et il lui a promis une présentation détaillée dans les quelques mois suivants.

Eh bien, la loi pertinente a été promulguée, le règlement sur le partage de l'information et l'utilisation du NAS a été adopté, et le Commissaire attend toujours la «présentation détaillée» promise. En fait, ce n'est qu'à la fin de 1990 que Revenu Canada a commencé à se pencher sur les implications du couplage des données pour la protection de la vie privée. Le Commissariat l'a pressé de lui fournir des détails, mais sans succès.

Retrait d'un projet de couplage de répertoires des permis de pêche et des permis de conduire des véhicules

Pêches et Océans a abandonné un projet grâce auquel il voulait renforcer sa capacité d'application de la réglementation des pêches en couplant les répertoires des détenteurs de permis de pêche avec ceux des titulaires des permis de conduire des «véhicules» utilisés pour la pêche. Le Ministère a retiré sa proposition quand il est devenu évident que rien dans la Loi ne pouvait justifier le couplage envisagé.

Couplage des dossiers médicaux des immigrants

Santé et Bien-être social Canada a soumis au Commissariat une proposition en vue d'évaluer l'état de santé global des immigrants grâce à un couplage des fichiers de ses services de santé (de l'Immigration) avec les fichiers médicaux provinciaux.

Le ministère ne voulait extraire de ces fichiers que des données statistiques, et il s'est engagé à ne pas s'en servir à des fins administratives.

En théorie, il n'est pas nécessaire que le Commissaire approuve un couplage comme celui-là, mais le Commissariat sait gré aux responsables de la Santé de l'en avoir informé. En effet, dans ce secteur, les données sont de nature si délicate que leur couplage continue à inquiéter le Commissaire.

Collecte de renseignements par le Service correctionnel du Canada

Le SCC a informé le Commissariat qu'il comptait améliorer ses méthodes de collecte de «renseignements critiques» sur les personnes qui allaient bientôt s'ajouter à la population carcérale. La nécessité de disposer de renseignements de meilleure qualité lui était sautée aux yeux après que deux personnes récemment libérées de pénitenciers fédéraux aient commis des meurtres à Toronto.

Quand un détenu arrive dans un établissement correctionnel, le SCC demande des renseignements à la police, aux tribunaux et à divers organismes carcéraux et services de libérations conditionnelles. Ces sources n'accordent pas toujours une grande priorité aux demandes du SCC, qui risque par conséquent de ne pas avoir certains renseignements d'importance critique pour déterminer à quel niveau de sécurité le détenu doit être classé ou quelles sont ses possibilités de libération conditionnelle. C'est dans la Région métropolitaine de Toronto que le problème est le plus aigu.

Par conséquent, le SCC se proposait de passer un marché avec d'anciens policiers de Toronto, qui se seraient chargés de recueillir les renseignements nécessaires.

Le Commissariat a étudié les contrats pour s'assurer qu'ils contenaient des dispositions satisfaisantes sur la collecte et l'utilisation des renseignements personnels recueillis par les contractuels, que la procédure de collecte elle-même était conforme à la *Loi sur la protection des renseignements personnels*, et que les renseignements recueillis seraient tous conservés dans une banque de données et mis à la disposition des personnes concernées. Le SCC a tenu compte de tous ces points.

Par ailleurs, le Commissariat a souligné que la divulgation de ces renseignements à des organismes provinciaux pourrait nécessiter leur examen par les homologues provinciaux du Commissaire. Il a aussi recommandé qu'on rédige des protocoles d'entente fédérale-provinciale pour régir les éventuels échanges de renseignements.

Répertoire des étudiants étrangers de l'ACDI

Le projet de l'Agence canadienne de développement international (ACDI) d'établir un répertoire des étudiants de l'étranger qu'elle subventionne continue à causer des difficultés au Commissariat.

Comme les dossiers de l'ACDI sont classés par projet ou par pays, il est difficile d'y retrouver les nom et adresse des étudiants en question. Pour se faciliter la tâche, l'ACDI se proposait de mettre sur pied un système de repérage fondé sur un couplage de ses fichiers avec ceux des autorisations délivrées aux étudiants par Emploi et Immigration, qui contiennent les renseignements nécessaires. À cette fin, l'ACDI comptait envoyer un fonctionnaire faire des recherches dans les fichiers d'EIC.

Bien que le personnel du Commissariat lui ait fait remarquer que rien dans la Loi ne pouvait justifier ce couplage, l'ACDI a soumis une proposition officielle au Commissaire. Au cours des discussions qui ont suivi, le personnel du Commissariat s'est bien rendu compte qu'on n'avait pas dit grand-chose sur la proposition aux fonctionnaires d'EIC, qui n'arrivaient pas non plus à trouver une justification juridique du couplage. Bref, ils n'avaient pas l'intention d'obtempérer à la demande de l'ACDI.

L'ACDI a donc demandé un plus long délai de consultation. Depuis, elle a soumis deux autres propositions. L'analyse du couplage proposé a révélé une anomalie : l'ACDI ne mentionne dans le guide InfoSource aucun fichier de renseignements personnels sur les étudiants et stagiaires. Le Commissariat en a informé le Conseil du Trésor, qui est chargé de veiller à ce que les organismes gouvernementaux respectent la *Loi sur la protection des renseignements personnels*.

Perception des dettes à même les remboursements d'impôt

L'utilisation par l'administration fédérale du NAS pour identifier ceux qui lui doivent de l'argent et pour déduire son dû de leurs remboursements d'impôt est sans doute l'un des plus vieux exemples de couplage de données.

En juin 1990, le Bureau du Contrôleur général a proposé un projet de recherche en vue d'évaluer l'utilité d'un programme de ce genre pour récupérer une partie des millions de dollars de prêts aux étudiants non remboursés. Le Commissariat a accepté qu'on fasse un couplage de données à des fins de recherche, en maintenant toutefois que l'État ne devrait pas retenir d'argent sur les remboursements d'impôt des contribuables à moins que la loi ne soit modifiée au préalable.

Le Commissariat voulait aussi qu'on l'assure qu'il n'y aurait pas de déduction à même les remboursements simplement parce que le même nom aurait figuré dans les deux fichiers couplés. En effet, dans les cas de couplage de données, une vérification indépendante s'impose avant que des mesures administratives quelconques soient prises.

Il n'avait pas encore été possible de rapprocher ces points de vue divergents en février 1991, quand le Gouvernement a déposé son budget. Néanmoins, on a fait allusion à cette occasion-là à des changements susceptibles de permettre à l'administration fédérale de récupérer son argent à même les remboursements d'impôt.

Il semble que les contribuables visés seront dûment prévenus et qu'on prendra grand soin de ne pas leur faire subir de trop grandes difficultés financières en raison de ce qu'on déduira de leurs remboursements d'impôt.

Cela dit, le Commissariat persiste à croire que ce genre de recouvrement des dettes des contribuables ne peut se faire sans modification de la loi. Il ne suffit pas d'invoquer la *Loi sur la gestion des finances publiques* ou de dire qu'un couplage de données de ce genre constitue une utilisation des renseignements «compatible» avec les fins auxquelles ceux-ci ont été recueillis, ou que leur divulgation est «pour des raisons d'intérêt public».

La technologie continue à progresser

Emploi et Immigration (EIC) est le fer de lance de la technologie des systèmes dans le milieu de travail. Et ce n'est pas surprenant, étant donné qu'EIC sert quelque 3 millions de prestataires de l'assurance-chômage, reçoit environ 40 millions de rapports de demandeurs et répond à plus de 30 millions de demandes de renseignements par année.

Cartes à mémoire

EIC a informé le Commissariat de son intention de lancer un projet pilote de cartes à mémoire qui seraient remises aux clients de l'assurance-chômage. Ces cartes, qui ressemblent beaucoup à des cartes bancaires ou à des cartes de crédit, sont en fait des mini-ordinateurs dotés d'une mémoire de 64 Kb, ce qui les rend aussi puissants que certains des premiers ordinateurs personnels. Les clients qui demandent des prestations en recevraient une, dont ils se serviraient pour signaler leurs périodes de chômage par l'intermédiaire de machines accessibles au public et reliées aux ordinateurs centraux d'EIC, qui détermineraient leur admissibilité, calculeraient leurs prestations et porteraient le montant à leur compte, sur la carte. Les demandeurs pourraient ensuite utiliser leur carte pour retirer de l'argent d'un guichet automatique ou pour faire des achats aux endroits équipés de machines à débit direct.

Le projet pilote devrait commencer en deux endroits à l'automne de 1991.

Dans ce contexte, il y a deux risques manifestes pour la vie privée. Le premier, c'est qu'il faut s'assurer que c'est bien la bonne personne qui a accès au système, et le second, qu'on doit prévenir tout couplage des données utilisées pour le système avec d'autres renseignements personnels qui n'y sont pas liés.

Le premier de ces risques semble avoir été évité. En effet, les clients auront accès au système grâce à un numéro d'identification personnel (NIP) de leur choix. De plus, EIC a prévu une protection interne si poussée qu'il la juge impénétrable. La sécurité du système sera d'ailleurs surveillée étroitement durant le projet pilote, et EIC informera le Commissaire des résultats obtenus à cet égard.

Le second danger sera prévenu grâce à une bonne protection contre les couplages indésirables de données. La carte ne pourra pas être utilisée pour d'autres opérations, et les machines utilisées dans les banques et chez les détaillants n'accepteront que les fonds correspondant à la transaction effectuée.

Néanmoins, EIC croit que la carte pourrait avoir jusqu'à huit applications différentes. Par exemple, elle pourrait relier son détenteur à une base de données électroniques de recherche d'emplois contenant des descriptions des emplois disponibles correspondant à sa formation et à son expérience. Elle pourrait aussi être utilisée pour vérifier et payer les indemnités de formation du détenteur et pour l'inscrire à des programmes de formation.

Avec autant d'applications possibles, les cartes seraient utiles pour d'autres ministères et organismes gouvernementaux, voire pour des entreprises privées. EIC pourrait vendre la capacité inutilisée, qui serait employée pour stocker des données ou pour faire des transactions financières. EIC reconnaît que, dans un contexte d'applications multiples, il faudrait distinguer très nettement les fonctions pour éviter toute fusion ou transfert de données d'un programme à l'autre.

Une grande partie du projet en est encore au stade de la conception. EIC estime qu'il lui faudra de trois à quatre ans pour lancer la partie du programme applicable à l'assurance-chômage, trois à quatre ans de plus pour la mettre entièrement en oeuvre et dix bonnes années pour que toutes les applications soient opérationnelles. L'ampleur du projet pourrait d'ailleurs nécessiter des modifications de la loi constituant EIC. À cet égard, le Commissariat a proposé que les changements soient axés sur la protection de la carte et de ses applications éventuelles, plutôt que sur les dispositions nécessaires pour en autoriser l'utilisation.

Nouveau système de réponse téléphonique aux demandes de renseignements d'EIC

Le Système de réponse vocale automatisée (SRVA) d'EIC continue de soulever des inquiétudes au Commissariat. Il s'agit d'un projet pilote qui permettrait aux usagers du téléphone à clavier d'obtenir par téléphone de l'information d'ordre général sur l'assurance-chômage, voire des renseignements détaillés sur leurs demandes de prestation. Ils pourraient se servir de leur téléphone pour choisir telles ou telles options, et ils s'identifieraient en donnant leur numéro d'assurance sociale et leur date de naissance. Avec le SRVA, les ordinateurs seraient capables de répondre à des milliers d'appels «ordinaires».

Le Commissariat a appris l'existence du système quand une station radio de Québec lui a demandé si cette utilisation du NAS était bien autorisée. Il est certain qu'EIC peut se servir du NAS, qui a été conçu expressément aux fins de l'assurance-chômage. Toutefois, les NAS et les dates de naissance des gens sont des renseignements si répandus que d'autres que les intéressés risquent d'avoir accès au système, si ce sont les deux seules preuves d'identité exigées.

EIC a reconnu que ces deux «pièces» ne suffiraient peut-être pas et a donc étudié d'autres solutions : autorisations des clients ou reconnaissance par le système de leur numéro de téléphone ou d'un numéro d'identification personnel (NIP) choisi par eux, comme pour les cartes bancaires. La meilleure solution semble être l'utilisation d'un NIP, mais il aurait fallu un an pour y avoir recours, alors que le projet pilote était sur le point d'être lancé en Ontario. Les pressions internes augmentaient, le Conseil du Trésor avait approuvé le projet et le système allait très bientôt faire l'objet d'un appel d'offres; bref, EIC a décidé d'aller de l'avant sans plus attendre.

Le Commissaire a admis qu'EIC était plus en mesure que quiconque de décider comment se servir de cette technologie pour servir le public. Il a toutefois demandé que le projet soit reporté jusqu'à ce que le système soit doté de protections plus sûres, en faisant remarquer qu'EIC risquait de se retrouver dans l'embarras s'il fallait que des renseignements concernant un de ses clients soient divulgués à tort.

Il était malheureusement trop tard; le projet avait déjà gagné London et Peterborough. EIC est d'avis que cette expansion facilitera la mise au point du système à l'échelle nationale, avec une meilleure protection.

Consultations auprès du Commissaire

Le Commissariat est toujours ravi d'échanger de l'information avec ceux qui s'intéressent à l'avancement de la protection de la vie privée. Comme les demandes de renseignements débordent souvent son mandat, il fait alors office d'aiguilleur, en trouvant l'information ou en conseillant à l'intéressé de s'adresser à d'autres sources.

C'est ainsi que le personnel chargé de la recherche a répondu à des demandes de renseignements du nouveau Commissaire fédéral à la protection de la vie privée de l'Australie, qui voulait se renseigner sur les lignes directrices applicables à la recherche médicale au Canada, sur l'application de la politique fédérale de couplage de données à des activités destinées à faire respecter les lois, sur les données concernant la sécurité et le renseignement de sécurité et sur l'expérience acquise au Canada en matière de surveillance secrète.

Le Commissaire a d'ailleurs reçu d'autres demandes de renseignements des antipodes. Par exemple, le Comité sur la protection de la vie privée de la Nouvelle-Galles du Sud lui a demandé une évaluation globale de la *Loi sur la protection des renseignements personnels* et de l'expérience acquise par le Commissariat. Le Commissaire aux élections de l'Australie a pour sa part demandé des renseignements sur la protection que la loi canadienne accorde aux dénonciateurs (il n'y a aucune) et Telecom Australia a demandé à savoir comment on traite au Canada le service du contrôle des appels et de l'affichage du numéro de téléphone du correspondant et quels sont les codes de conduite des entreprises de télécommunications.

Le Secrétaire de l'Intérieur de Hong Kong, qui faisait des recherches sur la législation en matière de protection des renseignements, a demandé de l'information sur les systèmes d'enregistrement des ordinateurs et sur les licences d'exploitation des banques de données. Ces deux questions font l'objet en Europe de régimes stricts de protection de renseignements; celui qui est prévu par la British *Data Protection Act* est particulièrement strict. Comme la loi canadienne ne prévoit aucune mesure de protection de ce genre, notre correspondant de Hong Kong a dû être aiguillé ailleurs.

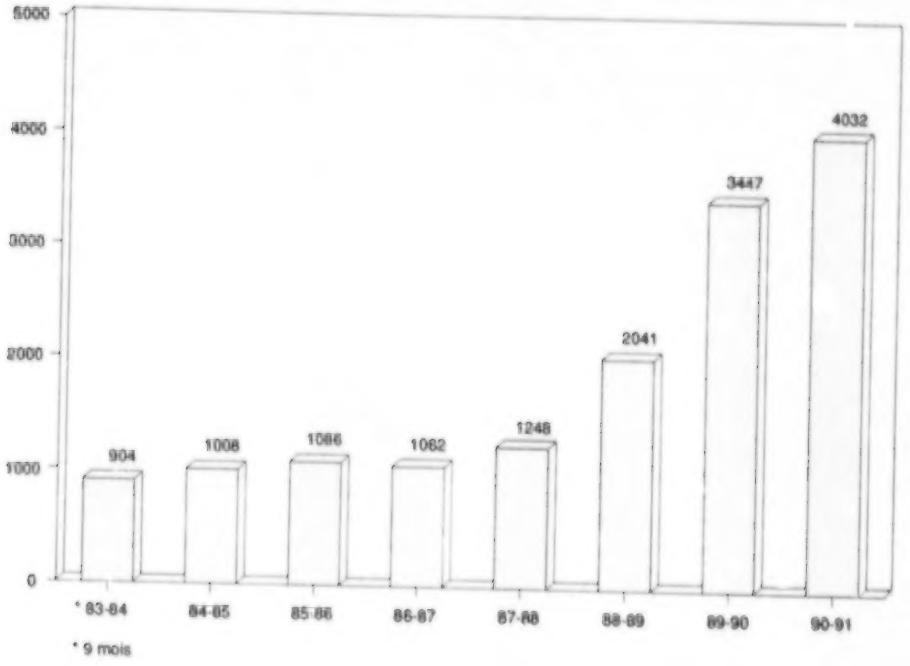
Le personnel du Commissariat a aussi fourni à ses homologues provinciaux de l'information de fond sur

- l'expérience acquise au niveau fédéral en matière de couplage de données (Ontario);
- et sur les implications pour la protection de la vie privée et l'appariement des registres de la santé et des services socio-économiques (Québec).

Enfin, le personnel a compilé les documents fédéraux les plus récents sur les applications informatiques des bases de données gouvernementales et mis sur pied des modalités de gestion de la distribution des bases de données des entreprises commerciales, en réponse à une demande du ministère ontarien de la Consommation et du Commerce sur les implications pour la protection de la vie privée des bases de données publiques.

La Commission royale d'enquête sur les nouvelles technologies de reproduction a demandé au Commissaire des commentaires sur les implications pour la protection de la vie privée des nouvelles techniques de reproduction. Le Commissaire compte présenter un document à ce sujet à la Commission royale, une fois que son étude sur les questions génétiques sera terminée. Pour le moment, il est heureux d'avoir été consulté.

Requêtes 1983-1991



* 9 mois

Demandes de renseignements

Le nombre de demandes de renseignements adressées au Commissariat continue d'augmenter. Au cours de l'année écoulée, il a reçu 4032 demandes par téléphone et par lettre, comparativement à 3447 l'an dernier, soit une augmentation de 17 p. 100.

La proportion des demandes d'interprétation de la Loi s'est élevée à 55 p. 100. Ces demandes sont très variées : par exemple, des employés de la Société canadienne des postes ont cherché à savoir s'ils étaient tenus de signer une formule de consentement à la divulgation de leurs dossiers médicaux à l'employeur, des détenus ont demandé si les pénitenciers pouvaient ouvrir leur courrier, et le bureau de l'accès à l'information et de la protection des renseignements personnels de Transports Canada a vérifié si la voix de quelqu'un, enregistrée sur bande audio, est considérée comme un renseignement personnel. Toutes ces demandes ont été acheminées au Conseil du Trésor ou au ministère de la Justice, pour interprétation.

La deuxième en importance des catégories des demandes de renseignements (17 p. 100) concerne des problèmes de protection de la vie privée qui ne relèvent pas de la compétence du Commissaire. Par exemple, 4 p. 100 des demandes ont trait à des organismes fédéraux et à des sociétés d'État qui ne sont pas assujettis à la Loi. Dans un cas, un agent du Service correctionnel du Canada a été secoué de constater qu'il apparaissait dans une émission télévisée par la Société Radio-Canada. Le caméraman lui aurait dit qu'il ne le filmait pas, mais qu'il ne faisait que régler son objectif. En raison de cette apparition à la télévision, l'intéressé craignait pour sa vie et pour celle d'autres gardes, car ils étaient parfois menacés par des détenus. Malheureusement étant donné que la Société Radio-Canada n'est pas assujettie à la Loi, le Commissariat n'a rien pu faire.

Une bonne partie des autres demandes (13 p. 100) porte sur d'autres paliers de gouvernement, et fréquemment sur le secteur privé. Ainsi, une femme a téléphoné au Commissariat au sujet d'une formule de demande d'emploi qui lui avait été remise par la Banque canadienne impériale de commerce (BCIC). Dans cette formule, la Banque lui demandait l'autorisation de faire divulguer des renseignements personnels sur elle par des organismes de crédit et par d'anciens employeurs. La formule contenait même une déclaration attestant que la permission que la signataire donnait s'appliquait à la divulgation de renseignements personnels la concernant au sens du paragraphe 8(2) de la *Loi sur la protection des renseignements personnels*.

Le personnel du Commissariat a dû vraiment se creuser la cervelle, d'abord parce que les banques ne sont pas assujetties à la Loi, puis parce que l'article 8 de la Loi dispose que les institutions fédérales ne peuvent pas communiquer de renseignements personnels sans le consentement de l'individu concerné. Le paragraphe mentionné dans la formule de la Banque précise les exceptions à la règle, mais aucune d'entre elles ne saurait être interprétée, même en étant tirée par les cheveux, comme autorisant la divulgation de ces renseignements à des employeurs éventuels!

Le Commissariat a conclu que l'attestation n'avait aucune valeur légale et ne réduisait nullement la protection des renseignements détenus par l'administration fédérale. Les conseillers juridiques du Commissariat et de la Banque ont discuté du consentement demandé par cette dernière, mais le Commissaire n'a pas pu faire retirer la déclaration contestée de la formule, étant donné qu'il n'a pas compétence dans le secteur bancaire. La Banque n'a hélas pas retiré la déclaration de son plein gré, car le Commissariat a reçu une autre plainte à cet égard.

Les demandes de renseignements les plus fréquentes au sujet du numéro d'assurance sociale (NAS) - 13 p. 100 de l'ensemble - concernent des compagnies d'assurance, des comptoirs de location de vidéos, des banques, des épiceries et des magasins à rayons. Nos correspondants sont à la fois étonnés et déçus de se faire dire que les utilisations du NAS ne sont limitées que dans l'administration fédérale.

Plusieurs de nos correspondants se sont dits très mécontents de la formule de demande de Carte d'or de la Banque royale, qui exige leur consentement à une collecte illimitée de renseignements et à la divulgation de leur NAS (s'ils l'ont déjà donné à la Banque dans une demande quelconque). Le Commissariat aimerait savoir si le fait d'ouvrir un compte bancaire constitue une «demande», étant donné que les clients doivent donner leur NAS à cette fin, conformément à la *Loi de l'impôt sur le revenu*.

Enfin, 8 p. 100 des demandes de renseignements n'ont aucun lien commun, si ce n'est que bon nombre d'entre elles concernent une éventuelle demande de pardon; celles-là sont renvoyées ailleurs. Une grande partie des autres proviennent de contribuables frustrés qui profitent de la possibilité d'appeler sans frais au Commissariat afin de pouvoir parler avec quelqu'un qui travaille pour le «Gouvernement».

Direction de l'observation

En 1990-1991, la Direction avait pour objectifs de faire des vérifications dans trois grandes institutions fédérales, d'évaluer et d'améliorer sa procédure de vérification - et la qualité de ses vérifications - , d'ajouter à sa démarche une sensibilisation des institutions à la protection de la vie privée et de mettre au point une méthode de vérification efficace à l'égard des renseignements personnels stockés dans des systèmes de traitement électronique des données.

La Direction a fait les trois vérifications qu'elle avait prévues, à la Défense nationale, à la Gendarmerie royale et aux Affaires extérieures, des institutions dont les banques de données contiennent des renseignements personnels très délicats et qui comptent parmi les plus complètes et les plus perfectionnées du Canada. La guerre du Golfe et la crise d'Oka ont quelque peu retardé les vérifications prévues au MDN et à la GRC, mais le personnel a quand même pu les mener à bien, en plus de produire un rapport provisoire sur la plus grande partie de la vérification réalisée aux Affaires extérieures.

En raison des problèmes logistiques et des frais de voyage considérables qu'elle aurait entraînés, la Direction a reporté sa vérification des activités des Affaires extérieures à l'étranger ainsi que son examen détaillé des systèmes de traitement de l'information internationale du Ministère. Ces modifications du calendrier de travail ont permis à la Direction d'entreprendre vers la fin de 1990 trois vérifications de moins grande envergure, l'une à la Commission de la capitale nationale, une autre au Bureau du Contrôleur général et la troisième au Commissariat aux langues officielles; seule la troisième était menée à bien à la fin de l'exercice.

Comme prévu, la Direction a ajouté à ses vérifications un volet de sensibilisation des institutions à la protection de la vie privée. Les équipes de vérification offrent dans les locaux des institutions visitées une explication de la *Loi sur la protection de la vie privée* étayée par la présentation de deux cassettes vidéo qui donnent une excellente idée de ce qu'elles cherchent à faire dans leurs vérifications. (Ces vidéos ne sont utilisées que si l'institution veut plus d'information.)

Toutes les vérifications de cette année ont compris une analyse améliorée des renseignements stockés dans les systèmes informatiques. Les nouvelles méthodes et la nouvelle approche ont été employées au MDN et à la GRC, ainsi qu'au Bureau du Contrôleur général. Dans ce dernier cas, la vérification a porté exclusivement sur le traitement électronique des données. L'expérience acquise rendra possible la production de manuels et de guides sur cet aspect de la vérification.

La Direction a aussi participé aux enquêtes ou projets spéciaux suivants :

- recherches sur toute la gamme des fréquences des téléphones cellulaires par la GRC;
- établissement par le SCRS d'un fichier inconsultable;
- vérification interne au ministère des Affaires indiennes et du Nord (MAIN);
- préoccupations soulevées par l'évaluation inversée au ministère de l'Industrie, des Sciences et de la Technologie ainsi qu'au MAIN;
- demande de divulgation des renseignements techniques détenus par Bell Canada au Service des renseignements (criminels) de l'Ontario.

CONSULTATIONS

Gendarmerie royale du Canada

Jusqu'à présent, les vérifications ont démontré que la GRC se distingue par la qualité de ses efforts concertés en vue de respecter la *Loi sur la protection des renseignements personnels*. En effet, elle accorde une priorité à ces questions, en organisant régulièrement des séances d'information à tous les niveaux et en incorporant une introduction à la *Loi sur la protection des renseignements personnels* au programme d'études des nouvelles recrues et des agents en formation.

Les vérificateurs ont constaté que, dans certains cas, les renseignements personnels détenus par la GRC n'étaient pas décrits convenablement dans le Répertoire des renseignements personnels (le nouvel InfoSource), mais il convient de souligner que ces lacunes étaient imputables à des oublis ou au fait que les descriptions n'avaient pas été modifiées pour refléter l'évolution des méthodes de fonctionnement de la Gendarmerie.

Certains dossiers contenant des renseignements personnels n'ont pas été retirés conformément aux calendriers établis et au règlement sur la protection de ces données. C'était particulièrement manifeste dans le cas des registres du rendement; ils ont fait l'objet de nombreuses rencontres entre le personnel du Commissariat et les responsables de la protection de la vie privée à la GRC, qui se sont tous efforcés de trouver une solution satisfaisant à la fois aux exigences de protection de la vie privée et aux contraintes administratives de la GRC.

Les vérificateurs ont jugé que, dans certains cas, les renseignements personnels n'étaient pas suffisamment bien protégés contre une divulgation non autorisée. Le cas le plus grave était celui du programme d'aide aux victimes, car les vérificateurs ont constaté que des conseillers bénévoles avaient eu accès à des dossiers d'enquête complets.

La vérification a révélé deux secteurs particulièrement intéressants, à savoir la transmission par télécopieur et l'utilisation de micro-ordinateurs pour le traitement des renseignements personnels. Nous sommes heureux de pouvoir conclure que la GRC s'est donnée une politique et une procédure de transmission de renseignements personnels par télécopieur et de traitement de ces renseignements par micro-ordinateurs. Grâce aux mécanismes de contrôle en place, la Gendarmerie ne peut transmettre des renseignements personnels de nature délicate que par l'intermédiaire des systèmes Comsec, d'une sécurité éprouvée. Les vérificateurs ont inspecté plusieurs systèmes informatiques utilisés par la GRC et ils ont constaté que, dans chaque cas, les renseignements personnels étaient bien protégés.

Ministère de la Défense nationale (MDN)

Le Commissariat a communiqué ses constatations détaillées au MDN, et il attend ses commentaires. Normalement, il ne rend pas ses constatations publiques avant que son personnel ait eu l'occasion d'étudier les commentaires de l'institution faisant l'objet de la vérification et de discuter de tous les points litigieux.

Autres vérifications

Les autres vérifications ont révélé, une fois de plus, que les normes de conservation et de retrait des renseignements personnels ne sont pas toujours respectées, voire qu'elles sont carrément insatisfaisantes. Les vérificateurs ont constaté que les dossiers du personnel ne sont généralement pas retirés en temps voulu, et que certains fichiers de renseignements personnels sont conservés indéfiniment. Les fichiers du personnel contiennent des renseignements sur des tiers qui risquent d'être divulgués par inadvertance. En outre, on trouve souvent dans certains fichiers du personnel des renseignements de nature délicate (ou non pertinents). Qui plus est, dans la plupart des institutions, le principe du «besoin de savoir» n'est pas appliqué. Beaucoup d'entre elles n'ont pas de méthodes de sécurité satisfaisantes pour protéger les renseignements personnels qu'elles détiennent, et la description de nombreux fichiers est incorrecte.

En toute justice, il faut reconnaître que la plupart des personnes rencontrées dans le contexte de nos vérifications ont dit s'intéresser non seulement aux objectifs de la vérification elle-même, mais aussi à une bonne application de la *Loi sur la protection des renseignements personnels* dans l'ensemble de l'institution à laquelle elles appartiennent. Dans plusieurs cas, les responsables ont même remédié aux problèmes avant le départ de nos vérificateurs.

Dans les petites institutions, qui ont moins de ressources que les grandes à consacrer à l'application de la Loi, il semble qu'on risque davantage de traiter incorrectement les renseignements personnels. Les politiques et procédures ont tendance à être désuètes ou totalement absentes, et le niveau global de connaissance de la Loi est toujours plus bas que dans les grands ministères et organismes. La sécurité des renseignements personnels recueillis par ces institutions est donc habituellement compromise.

C'est pour cette raison que nous sommes heureux de faire état de nos conclusions sur une petite institution qui traite généralement ses renseignements personnels conformément à la Loi.

Commissariat aux langues officielles

Durant toute notre vérification au Commissariat aux langues officielles, il était évident que, même si la plupart des employés n'avaient qu'une connaissance sommaire de la *Loi sur la protection des renseignements personnels*, tous étaient bien décidés à gérer convenablement les renseignements de ce genre. Les vérificateurs estiment d'ailleurs que ce souci reflète l'importance que la *Loi sur les langues officielles* accorde à la confidentialité des enquêtes sur les plaintes.

Néanmoins, les renseignements personnels que ce Commissariat détient ne sont pas toujours bien protégés contre leur divulgation non autorisée, et, dans un cas, la protection du système informatique laissait à désirer en raison d'une gestion et d'une protection insatisfaisantes des mots de passe.

Conclusions similaires

Globalement, l'exercice s'est soldé par une série d'observations communes à la plupart des vérifications.

Protection insuffisante des renseignements personnels

- Les cadres, superviseurs et autres employés sont autorisés à consulter les dossiers du personnel à des fins administratives courantes. Les préposés aux dossiers ont accès à leurs propres dossiers du personnel ainsi qu'à ceux de leurs collègues, ce qui leur donne la possibilité de prendre connaissance de renseignements personnels dont ils n'ont pas besoin pour leur travail (formules d'antécédents personnels, résultats des vérifications du crédit et des références, diagnostics médicaux, renseignements sur les membres de la famille, noms des bénéficiaires, achats de Bons d'épargne du Canada, contributions à Centraide, etc.).

- Certains dossiers de ce Commissariat contiennent quelques renseignements personnels sur des tiers, habituellement quand le nom de la personne visée figure avec ceux d'autres employés sur une liste où l'on trouve souvent le numéro d'assurance sociale de chacun.

- Les renseignements personnels traités par micro-ordinateurs ne sont généralement pas assez bien protégés, que ce soit par des moyens externes (verrouillage des claviers, protection du disque rigide, etc.) ou internes (comptes, codes d'identité, mots de passe, cloisonnements, sauvegardes, etc.).

- Les chemises contenant les dossiers tendent à porter une inscription contenant des détails sur l'intéressé en plus du titre du dossier. C'est particulièrement important lorsqu'il s'agit d'un dossier d'enquête ou de plainte, ou encore d'une demande spéciale.

Divulgation abusive de renseignements personnels

- Les dossiers du personnel contiennent souvent des documents qui auraient dû être carrément retirés, ou conservés dans d'autres dossiers. Les vérificateurs ont trouvé des renseignements médicaux ainsi que de l'information liée à la sécurité dans quelque 10 p. 100 des dossiers examinés.

Utilisation abusive des renseignements personnels

- Les renseignements personnels recueillis légalement à des fins précises sont parfois utilisés ensuite à d'autres fins (p. ex., des dossiers de harcèlement personnel utilisés dans des cas de griefs et de plaintes de discrimination).

Conservation et retrait insatisfaisants

- Les périodes de conservation et les calendriers de retrait de nombreux fichiers ne sont pas conformes aux règles et ne sont pas respectés.

Gestion intégrée

La gestion intégrée fournit au Commissariat à l'information et au Commissariat à la protection de la vie privée des services en matière de finances, de personnel, d'administration, d'informatique et de bibliothèque.

Finances

Le budget total des deux Commissariats pour l'année financière 1990-1991 s'élevait à 6 324 000 $. L'effectif global était de 78 années-personnes. Les augmentations étaient respectivement de 468 000 $ et de trois années-personnes par rapport à 1989-1990. Les dépenses engagées au titre du personnel (4 498 218 $) et des services professionnels et spéciaux (577 300 $) représentent plus de 87 p. 100 du total des dépenses. Le reste, soit 852 089 $, a couvert tous les autres frais.

Ci-dessous les dépenses des commissariats pour la période allant du 1er avril 1990 au 31 mars 1991*

	Information	Vie privée	Gestion intégrée	Total
Salaires	1 685 327	1 856 590	652 525	4 194 442
Contributions aux régimes d'avantages sociaux des employés	288 230	323 380	91 390	703 000
Transports et communications	38 141	114 167	123 309	275 617
Information	84 446	58 546	5 549	148 541
Services professionnels et spéciaux	411 801	130 150	35 349	577 300
Locations	3 952	2 214	11 413	17 579
Achats de services de réparation et d'entretien	14 628	3 919	9 676	28 223
Services publics, fournitures et approvisionnements	9 847	14 978	30 655	55 480
Acquisition de machines et d'équipement	176 326	51 508	85 672	313 416
Autres dépenses	6 145	3 475	3 584	13 204
TOTAL	2 718 753	2 558 927	1 049 122	6 326 802

* Les dépenses n'incluent pas les ajustements de fin d'année reflétés dans la section des comptes publics 1990-1991 traitant des commissariats.

État des dépenses des Commissariats pour la période du 1er avril 1990 au 31 mars 1991*

Personnel

Avec une augmentation nette de l'effectif de trois années-personnes et la nomination d'un nouveau Commissaire à la protection de la vie privée et d'un nouveau Commissaire à l'information, le programme du personnel a été fort occupé. Le nombre de mesures de dotation s'est élevé à 45, ce qui comprend les activités de recrutement externe, les cas d'avancement, l'embauchage de personnes nommées pour une période déterminée et certains cas de reclassification.

Administration

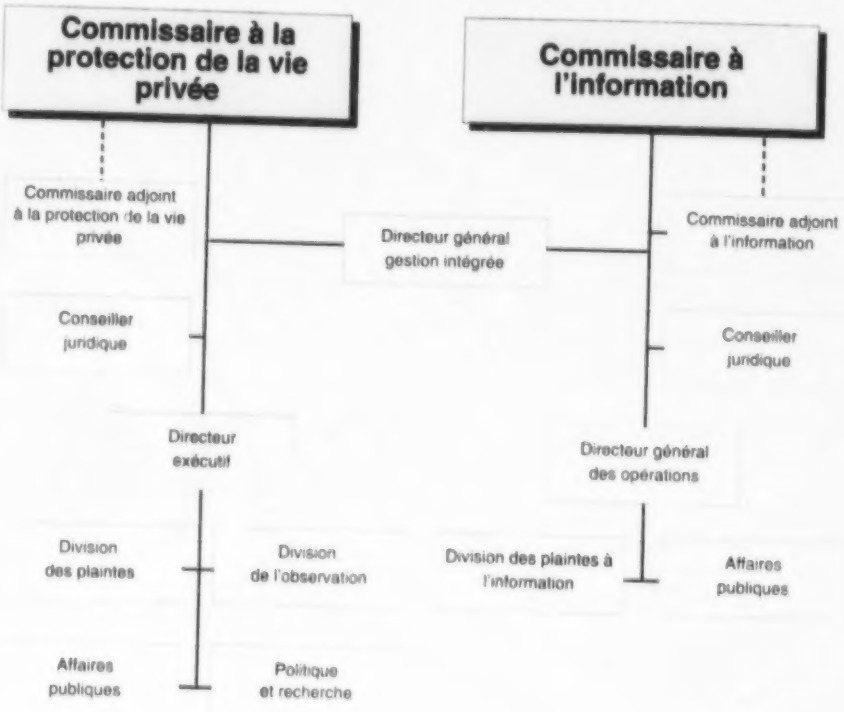
De nouveaux locaux ont été aménagés à l'automne de 1990, et certains progrès ont été accomplis dans le domaine de la gestion des documents, particulièrement pour l'établissement de calendriers de traitement des dossiers administratifs.

Informatique

Une nouvelle infrastructure informatique a été introduite. Le personnel a entrepris trois études, l'une sur les systèmes de gestion des affaires, l'autre sur la bureautique et la dernière sur les façons de travailler en milieu protégé. Les trois études seront menées à bien en 1991-1992 et produiront l'information nécessaire pour l'élaboration d'un plan à long terme de technologie informatique.

Bibliothèque

Les services de la bibliothèque sont à la disposition des deux commissaires ainsi que de leur personnel, mais le public y a aussi accès.

Les nouvelles acquisitions, effectuées grâce au Service du Programme de dépôt, totalisent 436 livres, périodiques et rapports annuels. La bibliothèque a prêté 835 ouvrages et répondu à 847 questions grâce à son service de référence. De plus, l'automatisation de ses services a été menée à bien.

Organigramme